

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année)

29 août 2000 (29.08.00)

Demande internationale no

PCT/FR00/00190

Référence du dossier du déposant ou du mandataire

5972.WO

Date du dépôt international (jour/mois/année)

27 janvier 2000 (27.01.00)

Date de priorité (jour/mois/année)

27 janvier 1999 (27.01.99)

Déposant

GUILLOU, Louis etc

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

19 juillet 2000 (19.07.00)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection



a été faite



n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Formulaire PCT/IB/331 (juillet 1992)

Fonctionnaire autorisé

Henrik Nyberg

no de téléphone: (41-22) 338.83.38

FR0000190

BEST AVAILABLE COPY

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

9/889918

Applicant's or agent's file reference 5972.WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/00190	International filing date (day/month/year) 27 January 2000 (27.01.00)	Priority date (day/month/year) 27 January 1999 (27.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant FRANCE TELECOM		

RECEIVED
JUL 28 2002
TECHNOLOGY CENTER

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
 - This REPORT consists of a total of 7 sheets, including this cover sheet.
- ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 25 sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 19 July 2000 (19.07.00)	Date of completion of this report 04 April 2001 (04.04.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00190

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

- ☒ the international application as originally filed.
- ☐ the description, pages 1-50, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.
- ☐ the claims, Nos. 16(partie),17,18, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-15,16(partie), filed with the letter of 09 January 2001 (09.01.2001),
Nos. _____, filed with the letter of _____.
- ☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00190

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

The set of amended claims filed with the applicant's response to the written opinion does not include the second part of Claim 16 or Claims 17 and 18. The report is based on Claims 1 to 15 as amended, and 16 to 19 as originally filed.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00190

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

The invention relates to a method (Claim 1) and a system (Claims 6 and 11) for proving, to a verification entity, the authenticity of an entity and/or the integrity of a message associated with said entity, comprising the following sequential steps: the entity carries out a commitment process; the verification entity issues a challenge; the control entity issues a response and the verification entity verifies said response. The invention also relates to a verification device (Claim 15) using said method.

Prior art:

Document EP-A-0 311 470, cited in the application, describes a similar method wherein an entity designated as a "trusted authority" assigns an identity to each entity designated as "control" and calculates the RSA signature thereof; in the course of the personnalisation procedure, the trusted authority provides the identity and signature to the control, whereafter the control entity declares: "Here is my identity; I know the RSA signature thereof". The control thus providing proof of knowledge of the RSA signature of the stated identity without disclosing said signature. Using the RSA verification public key

distributed by the trusted authority, an entity designated as "verification entity" verifies that the RSA signature corresponds to the stated identity without seeing said signature. The mechanisms using this protocol take place without any "transfer of knowledge": the control entity does not know the RSA private key used by the trusted authority to sign a large number of identities.

The problem:

The use of RSA technology opens up the authentication method to so-called "multiplicative" attacks. Moreover, the workload involved in the arithmetic operations requires computation times that are far too high for smart card-type applications.

The invention:

The method does not use the RSA signature, and computes commitments R , challenges d and responses R on the basis of public/private keys G_i and Q_i , as defined by the features of Claim 1.

None of the documents cited in the international search report discloses or suggests the computation steps defined in Claim 1. In particular, document EP-A-0 792 044 (category X), although it relates to a challenge/response type authentication method, uses the RSA technology.

Therefore, the subject matter of Claim 1 involves an inventive step (PCT Article 33).

Independent Claims 6 and 11 are equivalent to Claim 1, and relate to systems comprising the control device computing the commitments, receiving the challenges and computing

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00190

the responses. They therefore meet, likewise, the requirements of PCT Article 33.

Independent Claim 15 relates to a control device which computes G_i and Q_i values as per the method of the invention. Since said computations are neither disclosed nor suggested by the cited documents, said claim also meets the requirements of PCT Article 33.

The other claims are dependent claims that also meet, as such, the PCT requirements of novelty and inventive step.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00190

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. The pending application mentioned on page 50 of the description has not been identified by the application or publication number thereof (PCT Guidelines, Chapter II-4.17).

2. The expression "in the case where the prover has transmitted...", "operation of...", "in the case where the verification entity..." in the dependent claims are used with no prior reference thereto in the wording of the claims.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The following claims do not entirely meet the requirements of PCT Article 6 for the following reasons:

1. Independent Claim 1:

Since the verification step by the "verification" entity is not mentioned in the claim, the designation of the subject matter of the invention ("a method for proving to a verification entity the authenticity of an entity and/or the integrity of a message") is unclear: the features set forth in the claim relate solely to the computation of the commitment/challenge/response values usable in the authentication method of the invention.

2. Independent Claims 6 and 11 contain the same features as Claim 1, but expressed in terms of a system. The objection raised in paragraph 1 above also applies to these claims.

Moreover, although Claims 6 and 11 have been drafted in the form of separate independent claims, in fact they have the same subject matter and only differ from one another in terms of a variation in the definition of the subject matter for which protection is sought (a system comprising the control entity or a terminal device comprising the control entity). Consequently, said claims, taken as a whole, are not concise (PCT Article 6).

3. Independent Claim 15 relates to a verification device to be used with the terminal or control device. However, instead of device or system features, said claim comprises

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00190

VIII. Certain observations on the international application

method or process features, some of which are external to the claimed system ("unknown to the verification device").

09/889,918 8+T

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 09 APR 2001

WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)


Référence du dossier du déposant ou du mandataire 5972.WO	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00190	Date du dépôt international (jour/mois/année) 27/01/2000	Date de priorité (jour/mois/année) 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

- Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
- Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.
 - ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 25 feuilles.

- Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 19/07/2000	Date d'achèvement du présent rapport 04.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00190

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-50 version initiale

Revendications, N°:

16 (partie), 17, version initiale
18

1-15, reçue(s) le 10/01/2001 avec la lettre du 09/01/2001
16 (partie)

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00190

- ☐ de la description, pages :
☐ des revendications, n°s :
☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :
voir feuille séparée

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-18 Non : Revendications
Activité inventive	Oui : Revendications 1-18 Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-18 Non : Revendications

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point I**Base du rapport**

Le jeu de revendications amendées déposé avec la réponse du déposant à l'opinion écrite ne comprends pas la deuxième partie de la revendication 16 ni les revendications 17 et 18. Le rapport est basé sur les revendications 1 à 15 telles qu'amendées et 16 à 18 telles que dans la version initiale.

Concernant le point V**Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

L'invention concerne un procédé (revendication 1) et un système (revendications 6 et 11) destinés à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité, comportant les étapes successives d'engagement effectuée par l'entité, de défi effectué par le contrôleur, de réponse par le témoin et de contrôle par le contrôleur. Elle concerne aussi un dispositif contrôleur (revendication 15) utilisant ce procédé.

Etat de la technique:

EP-A-0 311 470, cité dans la demande, décrit un tel procédé selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par suite, le témoin proclame: "Voici mon identité; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le procédé d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques entraîne des temps de calculs trop importants pour les applications type carte à puce.

Invention:

Le procédé n'utilise pas la signature RSA et calcule des engagements R , défis d et réponses R à partir de valeurs publiques /privées G_i et Q_i définis selon les caractéristiques de la revendication 1.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les étapes de calcul définies dans la revendication 1. En particulier, EP-A-0 792 044 (cat. X) se rapporte aussi à un procédé d'authentification par défi/réponse, mais utilisant la technologie RSA.

L'objet de la revendication 1 implique par conséquent une activité inventive (article 33 PCT).

Les revendications indépendantes 6 et 11 correspondent à la revendication 1 en termes de systèmes comportant le dispositif témoin calculant les engagements, recevant les défis et calculant les réponses. Elles remplissent donc aussi les conditions de l'article 33 PCT.

La revendication indépendante 15 est relative à un dispositif contrôleur utilisant les calculs de G_i et Q_i propres au procédé de l'invention. Ces calculs n'étant ni divulgués ni suggérés par les documents cités, cette revendication remplit aussi les conditions de l'article 33 PCT.

Les autres revendications sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII

Irrégularités dans la demande internationale

1. La demande pendante évoquée à la page 50 de la description n'est pas identifiée par son numéro de demande ou de publication (Directives PCT, II 4.17).
2. Les expressions "cas où le démonstrateur a transmis ...", "opération de ...", "cas où le contrôleur..." dans les revendications dépendantes sont utilisées sans lien avec le reste du texte des revendications.

Concernant le point VIII

Observations relatives à la demande internationale

Les revendications suivantes ne remplissent pas entièrement les conditions de l'article 6 PCT pour les raisons suivantes:

1. revendication indépendante 1:

L'étape de contrôle par l'entité "contrôleur" n'étant pas indiquée dans la revendication, la désignation de l'objet de l'invention ("procédé destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message") n'est pas claire, les caractéristiques énoncées dans la revendication se rapportant uniquement aux calculs des valeurs d'engagements/défis/réponses utilisables dans le procédé d'authentification selon l'invention.

2. Les revendications indépendantes 6 et 11 contiennent les mêmes caractéristiques que la revendication 1 mais exprimées en terme de système. L'objection mentionnée au paragraphe 1 ci-dessus est donc aussi valable pour ces revendications.

De plus, bien que les revendications 6 et 11 aient été rédigées sous forme de revendications indépendantes distinctes, elles ont en fait le même objet et ne diffèrent l'une de l'autre que par une variation minimale dans la définition de l'objet pour lequel la protection est demandée (système comportant le témoin ou

dispositif terminal comportant le témoin). Par conséquent ces revendications, considérées ensemble, ne sont pas concises (Article 6 PCT).

3. La revendication indépendante 15 se rapporte à un dispositif contrôleur destiné à coopérer avec le dispositif terminal ou témoin. Elle ne comporte cependant aucune caractéristique de dispositif ou système mais des caractéristiques de méthode ou procédé, dont certaines sont de plus des caractéristiques extérieures au système revendiqué ("inconnus du dispositif contrôleur").

Revendications

1. Procédé destiné à prouver à une entité contrôleur,
 - l'authenticité d'une entité et/ou
 - l'intégrité d'un message **M** associé à cette entité,

5 au moyen :

- de **m** couples de valeurs privées **Q₁, Q₂, ... Q_m** et publiques **G₁, G₂, ... G_m**, **m** étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public **n** constitué par le produit de **f** facteurs premiers **p₁, p₂, ... p_f**, **f** étant supérieur ou égal à 2 ;

10 ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n};$$

v désignant un exposant public tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

15 ladite valeur publique **G_i** étant le carré **g_i²** d'un nombre de base **g_i** inférieur aux **f** facteurs premiers **p₁, p₂, ... p_f** ; le nombre de base **g_i** étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

20 n'a de solution en **x** dans l'anneau des entiers modulo **n** et tel que :

l'équation :

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en **x** dans l'anneau des entiers modulo **n** ;

25 ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des **f** facteurs premiers **p_i** et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées **Q_i** et/ou des **f.m** composantes **Q_{i,j}** (**Q_{i,j} ≡ Q_i mod p_j**) des valeurs privées **Q_i** et de l'exposant public **v** ;

- le témoin calcule des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

5 où r est un aléa tel que $0 < r < n$,

- soit

- en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

10 où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_t\}$,

- puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi d une réponse D ,

- 15 • soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

- 20 •• puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses D que de défis d que d'engagements R , chaque groupe de nombres R, d, D constituant un triplet noté $\{R, d, D\}$.

25 2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- étape 1 : acte d'engagement R

- à chaque appel, le témoin calcule chaque engagement R en appliquant le

processus spécifié selon la revendication 1,

- le démonstrateur transmet au contrôleur tout ou partie de chaque engagement R ,

• **étape 2 : acte de défi d**

5 - le contrôleur, après avoir reçu tout ou partie de chaque engagement R , produit des défis d en nombre égal au nombre d'engagements R et transmet les défis d au démonstrateur,

• **étape 3 : acte de réponse D**

10 - le témoin calcule des réponses D à partir des défis d en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse D au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où le démonstrateur a transmis une partie de chaque engagement
15 R , le contrôleur, disposant des m valeurs publiques $G_1, G_2, \dots G_m$, calcule à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots G_m^{d_m} \cdot D^v \text{ mod } n$$

ou a une relation du type,

20
$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots G_m^{d_m} \cdot \text{mod } n,$$

le contrôleur vérifie que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R qui lui a été transmis,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

25 dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement R , le contrôleur, disposant des m valeurs publiques $G_1, G_2, \dots G_m$, vérifie que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots G_m^{d_m} \cdot D^v \text{ mod } n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

- le démonstrateur transmet le jeton **T** au contrôleur,

- le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

- le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**,

- puis le contrôleur vérifie que le jeton T' est identique au jeton T transmis.

4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message M par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;

5 **Opération de signature**

ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message M ,
- les défis d et/ou les engagements R ,
- 10 - les réponses D ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

 • **étape 1 : acte d'engagement R**

15 - à chaque appel, le témoin calcule chaque engagement R en appliquant le processus spécifié selon la revendication 1,

 • **étape 2 : acte de défi d**

- le signataire applique une fonction de hachage h ayant comme arguments le message M et chaque engagement R pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis d en nombre égal au
20 nombre d'engagements R ,

 • **étape 3 : acte de réponse D**

- le témoin calcule des réponses D à partir des défis d en appliquant le processus spécifié selon la revendication 1.

25 5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message M en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit :

• cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

dans le cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

- 5 • • le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- 10 • • le contrôleur vérifie que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

• cas où le contrôleur dispose des défis **d** et des réponses **D**

dans le cas où le contrôleur dispose des défis **d** et des réponses **D**,

- 15 • • le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- 20 • • le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• cas où le contrôleur dispose des engagements **R** et des réponses **D**

dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**,

- 25 • • le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(\text{message}, R)$$

• • le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{mod } n$$

6. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou

- l'intégrité d'un message M associé à cette entité,

au moyen :

- de m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques $G_1, G_2,$

\dots, G_m , m étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,

- d'un module public n constitué par le produit de f facteurs premiers

p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{mod } n \text{ ou } G_i \equiv Q_i^v \text{mod } n ;$$

v désignant un exposant public tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

$$x^2 \equiv g_i \text{mod } n \quad \text{et} \quad x^2 \equiv -g_i \text{mod } n$$

n'a de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \text{mod } n$$

a des solutions en x dans l'anneau des entiers modulo n ;

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

le dispositif témoin comporte

- une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public v ;

ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

5 il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

7. Système selon la revendication 6 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ledit système étant tel qu'il comporte

10 - un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

15 - un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;
20 ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

25

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

5 • **étape 2 : acte de défi d**

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**,

10 le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

 • **étape 3 : acte de réponse D**

15 les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

 • **étape 4 : acte de contrôle**

20 les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

25 - des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif

contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , calculent à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit R' à tout ou partie de chaque engagement R reçu, cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement R , les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , vérifient que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

8. Système selon la revendication 6 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message M associé à une entité appelée démonstrateur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un

serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

5 ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements R du dispositif témoin calculent chaque engagement R en appliquant le processus spécifié selon la revendication 1,

10 le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement R au dispositif démonstrateur, via les moyens d'interconnexion,

• **étape 2 : acte de défi d**

15 le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage h ayant comme arguments le message M et tout ou partie de chaque engagement R, pour calculer au moins un jeton T,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-
20 après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton T, via les moyens de connexion, au dispositif contrôleur,

le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton T, des défis d en nombre égal au
25 nombre d'engagements R,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis d au démonstrateur, via les moyens de connexion ;

• **étape 3 : acte de réponse D**

les moyens de réception des défis d du dispositif témoin, reçoivent chaque défi d provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses D du dispositif témoin, calculent les réponses D à partir des défis d en appliquant le processus spécifié selon la revendication 1,

• étape 4 : acte de contrôle

les moyens de transmission du démonstrateur transmettent chaque réponse D au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , pour d'une part, calculer à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \text{ mod } n$$

puis d'autre part, calculer en appliquant la fonction de hachage h ayant comme arguments le message M et tout ou partie de chaque engagement reconstruit R' , un jeton T' ,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé T' au jeton T reçu.

9. Système selon la revendication 6 destiné à produire la signature numérique d'un message M , ci-après désigné le message signé, par une entité appelée entité signataire ;

le message signé comprenant :

- le message M ,
- les défis d et/ou les engagements R ,

- les réponses **D** ;

Opération de signature

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

• étape 1 : acte d'engagement **R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

• étape 2 : acte de défi **d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• étape 3 : acte de réponse **D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

5 **10.** Système selon la revendication 9 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

10 ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment

15 via un réseau de communication informatique, au dispositif signataire ; le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant :

- 20 - le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

le dispositif contrôleur comporte :

 - des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

25 - des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• **cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,**

dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis

d, des réponses **D**,

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$5 \quad R \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \bmod n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

10

$$d = h(\text{message}, R)$$

• cas où le dispositif contrôleur dispose des défis **d** et des réponses **D** dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**,

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

15

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \bmod n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

20

$$d = h(\text{message}, R')$$

• cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**

25 dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**,

• • les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(\text{message}, R)$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements R , les défis d' et les réponses D , satisfont à des relations du type :

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \text{ mod } n$$

11. Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à un dispositif contrôleur,

- l'authenticité de l'entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen :

- de m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots, G_m , m étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{ mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n ;$$

v désignant un exposant public tel que :

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites:

aucune des deux équations :

$$x^2 \equiv g_i \text{ mod } n \quad \text{et} \quad x^2 \equiv -g_i \text{ mod } n$$

n'a de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \text{ mod } n$$

a des solutions en x dans l'anneau des entiers modulo n ;

ledit dispositif terminal comprend un dispositif témoin comportant,

- une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) des valeurs privées Q_i et l'exposant public v ;

ledit dispositif témoin comporte aussi

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \text{ mod } n$$

ou r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^v \text{ mod } p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots \cdot Q_m^{dm} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \dots \cdot Q_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

12. Dispositif terminal selon la revendication 11 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

5 le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• étapes 2 et 3 : acte de défi **d**, acte de réponse **D**

10 les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin, les moyens de calcul des réponses **D** du dispositif témoin, calculent les
15 réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• étape 4 : acte de contrôle

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle,

20 13. Dispositif terminal selon la revendication 11 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,
ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant
25 interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,
ledit dispositif démonstrateur comportant des moyens de connexion pour le

connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur,

ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**,

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

5 les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

14. Dispositif terminal selon la revendication 11 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;

10 le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

15 ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

20 ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

25

Opération de signature

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement **R****

à chaque appel, les moyens de calcul des engagements **R** du dispositif

témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

• étape 2 : acte de défi **d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• étape 3 : acte de réponse **D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

15. Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur, destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen :

- de **m** couples de valeurs publiques **G₁, G₂, ... G_m**, **m** étant supérieur ou égal à 1,

- d'un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2, inconnus du dispositif contrôleur et de l'entité contrôleur associé ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$5 \quad G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n} ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i ,

v désignant un exposant public tel que

$$v = 2^k$$

10 où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

$$15 \quad x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'a de solution en x dans l'anneau des entiers modulo n

l'équation :

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n ;

20 16. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de
25 manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- étapes 1 et 2 : acte d'engagement R , acte de défi d

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, \dots, G_m , calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \text{mod } n,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu,

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 5972.WO	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00190	Date du dépôt international (jour/mois/année) 27/01/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 27/01/1999
Déposant FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

- ☐ le texte est approuvé tel qu'il a été remis par le déposant
- ☒ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

- ☐ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

☐ Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- m couples de valeurs privées Q_i et publiques P_i , $m > 1$
- un module public n constitué par le produit de f facteurs premiers p_i , $f > 2$.
- un exposant public v ,

liés par des relations du type:

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \quad \text{ou} \quad G_i \equiv Q_i^v \pmod{n}.$$

Ledit exposant v est tel que

$$v = 2^k$$

où $k > 1$ est un paramètre de sécurité.

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_i , tel que les deux équations:

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n , et tel que l'équation

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n .

RAPPORT DE RECHERCHE INTERNATIONALE

Document Internationale No
PCT/FR 00/00190

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27) colonne 9, ligne 39 - colonne 12, ligne 38 figure 3	1,6,11, 12,15 2,7,16
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24) page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30) page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6 -/-	3,4,8,9, 13,14, 17,18

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

28 mars 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Masche, C

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A ✓	EP 0 311 470 A (TELEDIFFUSION FSE ; FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 12, ligne 30 - colonne 13, ligne 55 ----	1,6,11, 15
A ✓	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 32 - ligne 61 -----	1,6,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/00190

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0792044	A	27-08-1997	JP 10247905 A	14-09-1998
			US 5987134 A	16-11-1999
WO 9633567	A	24-10-1996	FR 2733378 A	25-10-1996
			FR 2733379 A	25-10-1996
			EP 0766894 A	09-04-1996
			JP 10506727 T	30-06-1998
			US 5910989 A	08-06-1999
WO 8911706	A	30-11-1989	AU 622915 B	30-04-1992
			AU 3733589 A	12-12-1989
			CA 1321649 A	24-08-1993
			EP 0374225 A	27-06-1990
			JP 2504435 T	13-12-1990
			US 4935962 A	19-06-1990
EP 0311470	A	12-04-1989	FR 2620248 A	10-03-1989
			AT 83573 T	15-01-1993
			AU 2197188 A	23-03-1989
			CA 1295706 A	11-02-1992
			DE 3876741 A	28-01-1993
			FI 884082 A, B,	08-03-1989
			JP 1133092 A	25-05-1989
			KR 9608209 B	20-06-1996
			US 5218637 A	08-06-1993
			US 5140634 A	18-08-1992

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 5972.WO	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/00190	Date du dépôt international (jour/mois/année) 27/01/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 27/01/1999
Déposant FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.



Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.



la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :



contenu dans la demande internationale, sous forme écrite.



déposée avec la demande internationale, sous forme déchiffrable par ordinateur.



remis ultérieurement à l'administration, sous forme écrite.



remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.



La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.



La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2.



Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3.



Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,



le texte est approuvé tel qu'il a été remis par le déposant.



Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,



le texte est approuvé tel qu'il a été remis par le déposant



le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°



suggérée par le déposant.



parce que le déposant n'a pas suggéré de figure.



parce que cette figure caractérise mieux l'invention.



Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGÉ (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- m couples de valeurs privées Q_i et publiques P_i , $m > 1$
- un module public n constitué par le produit de f facteurs premiers p_i , $f > 2$.
- un exposant public v ,

liés par des relations du type:

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \quad \text{ou} \quad G_i \equiv Q_i^v \pmod{n}.$$

Ledit exposant v est tel que

$$v = 2^k$$

où $k > 1$ est un paramètre de sécurité.

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_i , tel que les deux équations:

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n , et tel que l'équation

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n .

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 00/00190

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A . A A	<p>EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27)</p> <p>colonne 9, ligne 39 -colonne 12, ligne 38 figure 3</p> <p style="text-align: center;">---</p> <p>WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24)</p> <p>page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17</p> <p style="text-align: center;">---</p> <p>WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30)</p> <p>page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/--</p>	<p>1,6,11, 12,15 2,7,16</p> <p>3,4,8,9, 13,14, 17,18</p> <p>3,4,8,9, 13,14, 17,18</p>

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

28 mars 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Masche, C

RAPPORT DE RECHERCHE INTERNATIONALE

ande Internationale No

PCT/FR 00/00190

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 311 470 A (TELEDIFFUSION FSE ; FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 12, ligne 30 - colonne 13, ligne 55 ---	1,6,11, 15
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 32 - ligne 61 -----	1,6,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/00190

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0792044	A	27-08-1997	JP 10247905 A	14-09-1998
			US 5987134 A	16-11-1999
W0 9633567	A	24-10-1996	FR 2733378 A	25-10-1996
			FR 2733379 A	25-10-1996
			EP 0766894 A	09-04-1996
			JP 10506727 T	30-06-1998
			US 5910989 A	08-06-1999
W0 8911706	A	30-11-1989	AU 622915 B	30-04-1992
			AU 3733589 A	12-12-1989
			CA 1321649 A	24-08-1993
			EP 0374225 A	27-06-1990
			JP 2504435 T	13-12-1990
			US 4935962 A	19-06-1990
EP 0311470	A	12-04-1989	FR 2620248 A	10-03-1989
			AT 83573 T	15-01-1993
			AU 2197188 A	23-03-1989
			CA 1295706 A	11-02-1992
			DE 3876741 A	28-01-1993
			FI 884082 A, B,	08-03-1989
			JP 1133092 A	25-05-1989
			KR 9608209 B	20-06-1996
			US 5218637 A	08-06-1993
			US 5140634 A	18-08-1992

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGÉE DE
LA RECHERCHE INTERNATIONALE

PCT

21 AVR. 2000

Destinataire

Cabinet Patrice VIDON
A l'att. de VIDON, P.
Immeuble Germanium
80 Avenue des Buttes de Coësmes
F-35700 Rennes
FRANCE

COPIE

NOTIFICATION DE TRANSMISSION DU
RAPPORT DE RECHERCHE INTERNATIONALE
OU DE LA DECLARATION

(règle 44.1 du PCT)

Référence du dossier du déposant ou du mandataire 5972.WO	Date d'expédition <i>(jour/mois/année)</i> 19/04/2000
Demande internationale n° PCT/FR 00/00190	Date du dépôt international <i>(jour/mois/année)</i> 27/01/2000
Déposant FRANCE TELECOM et al.	

1. ☒ Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.
Dépôt de modifications et d'une déclaration selon l'article 19 :
 Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand?	Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.
Où?	Directement auprès du Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.
2. ☐ Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2(a), est transmise ci-joint.
3. ☐ **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

☐ la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

☐ la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.
4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:
 Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90bis.1 et 90bis.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.
 Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).
 Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Hans Pettersson
---	--

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand?

Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment?

Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (Instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220 (suite)

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

- i) la revendication n'est pas modifiée;
- ii) la revendication est supprimée;
- iii) la revendication est nouvelle;
- iv) la revendication remplace une ou plusieurs revendications telles que déposées;
- v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."
2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
"Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."
3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."
4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendications 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 5972.W0	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/00190	Date du dépôt international (jour/mois/année) 27/01/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 27/01/1999
Déposant FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

- ☐ le texte est approuvé tel qu'il a été remis par le déposant
- ☒ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

- ☐ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

☐ Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABRÉGÉ (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- m couples de valeurs privées Q_i et publiques P_i , $m > 1$
- un module public n constitué par le produit de f facteurs premiers p_i , $f > 2$.
- un exposant public v ,

liés par des relations du type:

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \quad \text{ou} \quad G_i \equiv Q_i^v \pmod{n}.$$

Ledit exposant v est tel que

$$v = 2^k$$

où $k > 1$ est un paramètre de sécurité.

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_i , tel que les deux équations:

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n , et tel que l'équation

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n .

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

FR 00/00190

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27) colonne 9, ligne 39 -colonne 12, ligne 38 figure 3 ---	1,6,11, 12,15 2,7,16
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24) page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17 ---	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30) page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6 ---	3,4,8,9, 13,14, 17,18
	--- -/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

28 mars 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Masche, C

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

/FR 00/00190

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 12, ligne 30 -colonne 13, ligne 55 ----	1,6,11, 15
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 32 - ligne 61 -----	1,6,11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux familles de brevets

Demande Internationale No

FR 00/00190

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0792044 A	27-08-1997	JP 10247905 A	14-09-1998
		US 5987134 A	16-11-1999
WO 9633567 A	24-10-1996	FR 2733378 A	25-10-1996
		FR 2733379 A	25-10-1996
		EP 0766894 A	09-04-1996
		JP 10506727 T	30-06-1998
		US 5910989 A	08-06-1999
WO 8911706 A	30-11-1989	AU 622915 B	30-04-1992
		AU 3733589 A	12-12-1989
		CA 1321649 A	24-08-1993
		EP 0374225 A	27-06-1990
		JP 2504435 T	13-12-1990
		US 4935962 A	19-06-1990
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		FI 884082 A, B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: L'ADMINISTRATION CHARGÉE DE
L'EXAMEN PRELIMINAIRE INTERNATIONAL

09 AVR. 2001

PCT

Destinataire:

VIDON, P.
Cabinet Patrice VIDON
Immeuble Germanium
80 Avenue des Buttes de Coësmes
35700 Rennes
FRANCE

COPIE

NOTIFICATION DE TRANSMISSION DU
RAPPORT D'EXAMEN PRELIMINAIRE
INTERNATIONAL
(règle 71.1 du PCT)

Date d'expédition
(jour/mois/année) 04.04.2001

Référence du dossier du déposant ou du mandataire
5972.WO

NOTIFICATION IMPORTANTE

Demande internationale No.
PCT/FR00/00190

Date du dépôt international (jour/mois/année)
27/01/2000

Date de priorité (jour/mois/année)
27/01/1999

Déposant
FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.


4. RAPPEL

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Lorsqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'administration chargée de l'examen préliminaire international

 Office européen des brevets
D-80298 Munich
Tél. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Fonctionnaire autorisé

Barrio Baranano, A

Tél. +49 89 2399-8621




TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 5972.WO	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00190	Date du dépôt international (jour/mois/année) 27/01/2000	Date de priorité (jour/mois/année) 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		
<p>1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.</p> <p>2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.</p> <p><input checked="" type="checkbox"/> Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).</p> <p>Ces annexes comprennent 25 feuilles.</p>		
<p>3. Le présent rapport contient des indications relatives aux points suivants:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Base du rapport II <input type="checkbox"/> Priorité III <input type="checkbox"/> Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle IV <input type="checkbox"/> Absence d'unité de l'invention V <input checked="" type="checkbox"/> Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration VI <input type="checkbox"/> Certains documents cités VII <input checked="" type="checkbox"/> Irrégularités dans la demande internationale VIII <input checked="" type="checkbox"/> Observations relatives à la demande internationale 		
Date de présentation de la demande d'examen préliminaire internationale 19/07/2000	Date d'achèvement du présent rapport 04.04.2001	
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828	



RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00190

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-50 version initiale

Revendications, N°:

16 (partie), 17, version initiale
18

1-15, reçue(s) le 10/01/2001 avec la lettre du 09/01/2001
16 (partie)

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00190

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :
voir feuille séparée

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-18
	Non : Revendications
Activité inventive	Oui : Revendications 1-18
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-18
	Non : Revendications

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point I

Base du rapport

Le jeu de revendications amendées déposé avec la réponse du déposant à l'opinion écrite ne comprends pas la deuxième partie de la revendication 16 ni les revendications 17 et 18. Le rapport est basé sur les revendications 1 à 15 telles qu'amendées et 16 à 18 telles que dans la version initiale.

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) et un système (revendications 6 et 11) destinés à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité, comportant les étapes successives d'engagement effectuée par l'entité, de défi effectué par le contrôleur, de réponse par le témoin et de contrôle par le contrôleur. Elle concerne aussi un dispositif contrôleur (revendication 15) utilisant ce procédé.

Etat de la technique:

EP-A-0 311 470, cité dans la demande, décrit un tel procédé selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par suite, le témoin proclame: "Voici mon identité; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le procédé d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques entraîne des temps de calculs trop importants pour les applications type carte à puce.

Invention:

Le procédé n'utilise pas la signature RSA et calcule des engagements R , défis d et réponses R à partir de valeurs publiques /privées G_i et Q_i définis selon les caractéristiques de la revendication 1.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les étapes de calcul définies dans la revendication 1. En particulier, EP-A-0 792 044 (cat. X) se rapporte aussi à un procédé d'authentification par défi/réponse, mais utilisant la technologie RSA.

L'objet de la revendication 1 implique par conséquent une activité inventive (article 33 PCT).

Les revendications indépendantes 6 et 11 correspondent à la revendication 1 en termes de systèmes comportant le dispositif témoin calculant les engagements, recevant les défis et calculant les réponses. Elles remplissent donc aussi les conditions de l'article 33 PCT.

La revendication indépendante 15 est relative à un dispositif contrôleur utilisant les calculs de G_i et Q_i propres au procédé de l'invention. Ces calculs n'étant ni divulgués ni suggérés par les documents cités, cette revendication remplit aussi les conditions de l'article 33 PCT.

Les autres revendications sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII

Irrégularités dans la demande internationale

1. La demande pendante évoquée à la page 50 de la description n'est pas identifiée par son numéro de demande ou de publication (Directives PCT, II 4.17).
2. Les expressions "cas où le démonstrateur a transmis ...", "opération de ...", "cas où le contrôleur..." dans les revendications dépendantes sont utilisées sans lien avec le reste du texte des revendications.

Concernant le point VIII

Observations relatives à la demande internationale

Les revendications suivantes ne remplissent pas entièrement les conditions de l'article 6 PCT pour les raisons suivantes:

1. revendication indépendante 1:

L'étape de contrôle par l'entité "contrôleur" n'étant pas indiquée dans la revendication, la désignation de l'objet de l'invention ("procédé destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message") n'est pas claire, les caractéristiques énoncées dans la revendication se rapportant uniquement aux calculs des valeurs d'engagements/défis/réponses utilisables dans le procédé d'authentification selon l'invention.

2. Les revendications indépendantes 6 et 11 contiennent les mêmes caractéristiques que la revendication 1 mais exprimées en terme de système. L'objection mentionnée au paragraphe 1 ci-dessus est donc aussi valable pour ces revendications.

De plus, bien que les revendications 6 et 11 aient été rédigées sous forme de revendications indépendantes distinctes, elles ont en fait le même objet et ne diffèrent l'une de l'autre que par une variation minimale dans la définition de l'objet pour lequel la protection est demandée (système comportant le témoin ou

dispositif terminal comportant le témoin). Par conséquent ces revendications, considérées ensemble, ne sont pas concises (Article 6 PCT).

3. La revendication indépendante 15 se rapporte à un dispositif contrôleur destiné à coopérer avec le dispositif terminal ou témoin. Elle ne comporte cependant aucune caractéristique de dispositif ou système mais des caractéristiques de méthode ou procédé, dont certaines sont de plus des caractéristiques extérieures au système revendiqué ("inconnus du dispositif contrôleur").

Revendications

1. Procédé destiné à prouver à une entité contrôleur,
 - l'authenticité d'une entité et/ou
 - l'intégrité d'un message M associé à cette entité,

au moyen :

- de m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots, G_m , m étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n} ;$$

v désignant un exposant public tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'a de solution en x dans l'anneau des entiers modulo n et tel que :

l'équation :

$$x^v \equiv g_i^{2^k} \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n ;

ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des f facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public n et/ou des m valeurs privées Q_i et/ou des $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) des valeurs privées Q_i et de l'exposant public v ;

- le témoin calcule des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

5 où r est un aléa tel que $0 < r < n$,

- soit

- en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

10 où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$,

- puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi d une réponse D ,

15 • soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

20 •• puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses D que de défis d que d'engagements R , chaque groupe de nombres R, d, D constituant un triplet noté $\{R, d, D\}$.

25 2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- étape 1 : acte d'engagement R

- à chaque appel, le témoin calcule chaque engagement R en appliquant le

processus spécifié selon la revendication 1,

- le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R**,

• **étape 2 : acte de défi d**

5 - le contrôleur, après avoir reçu tout ou partie de chaque engagement **R**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

10 - le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où le démonstrateur a transmis une partie de chaque engagement
15 **R**, le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

ou a une relation du type,

20
$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n ,$$

le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

25 dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,

- le démonstrateur transmet le jeton **T** au contrôleur,

- le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

- le contrôleur, disposant des *m* valeurs publiques G_1, G_2, \dots, G_m , calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**,

- puis le contrôleur vérifie que le jeton T' est identique au jeton T transmis.

4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message M par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;

5 **Opération de signature**

ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message M ,
- les défis d et/ou les engagements R ,
- 10 - les réponses D ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

 • **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement R en appliquant le processus spécifié selon la revendication 1,

15 • **étape 2 : acte de défi d**

- le signataire applique une fonction de hachage h ayant comme arguments le message M et chaque engagement R pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis d en nombre égal au
- 20 nombre d'engagements R ,

 • **étape 3 : acte de réponse D**

- le témoin calcule des réponses D à partir des défis d en appliquant le processus spécifié selon la revendication 1.

5 5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message M en contrôlant, par une entité appelée contrôleur, le message signé;

25 **Opération de contrôle**

ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit :

• cas où le contrôleur dispose des engagements R , des défis d , des réponses D ,

dans le cas où le contrôleur dispose des engagements R , des défis d , des réponses D ,

- 5 • • le contrôleur vérifie que les engagements R , les défis d et les réponses D satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- 10 • • le contrôleur vérifie que le message M , les défis d et les engagements R satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le contrôleur dispose des défis d et des réponses D ,

- 15 • • le contrôleur reconstruit, à partir de chaque défi d et de chaque réponse D , des engagements R' satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- 20 • • le contrôleur vérifie que le message M et les défis d satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• cas où le contrôleur dispose des engagements R et des réponses D

dans le cas où le contrôleur dispose des engagements R et des réponses D ,

- 25 • • le contrôleur applique la fonction de hachage et reconstruit d'

$$d' = h(\text{message}, R)$$

• • le contrôleur vérifie que les engagements R , les défis d' et les réponses D , satisfont à des relations du type :

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{mod } n$$

6. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou

- l'intégrité d'un message M associé à cette entité,

au moyen :

- de m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques $G_1, G_2,$

\dots, G_m , m étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,

- d'un module public n constitué par le produit de f facteurs premiers

p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{mod } n \text{ ou } G_i \equiv Q_i^v \text{mod } n ;$$

v désignant un exposant public tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

$$x^2 \equiv g_i \text{mod } n \quad \text{et} \quad x^2 \equiv -g_i \text{mod } n$$

n'a de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \text{mod } n$$

a des solutions en x dans l'anneau des entiers modulo n ;

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

le dispositif témoin comporte

- une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public v ;

5 ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

15 • soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

20 ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

25 • soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

• soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

7. Système selon la revendication 6 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;
ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

5

• étape 2 : acte de défi **d**

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**,

10

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• étape 3 : acte de réponse **D**

15

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• étape 4 : acte de contrôle

20

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

25

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif

contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , calculent à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit R' à tout ou partie de chaque engagement R reçu,

cas où le démonstrateur a transmis l'intégralité de chaque engagement

R

dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement R , les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , vérifient que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

8. Système selon la revendication 6 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message M associé à une entité appelée démonstrateur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un

serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

5 ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

10 le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

• **étape 2 : acte de défi d**

15 le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-
20 après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur,

le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au
25 nombre d'engagements **R**,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• étape 4 : acte de contrôle

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

9. Système selon la revendication 6 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,

- les réponses **D** ;

Opération de signature

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

• **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

10. Système selon la revendication 9 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire ;

le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

- cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis

d, des réponses D,

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements R, les défis d et les réponses D satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message M, les défis d et les engagements R satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

• cas où le dispositif contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis d et des réponses D,

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi d et de chaque réponse D, des engagements R' satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message M et les défis d satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• cas où le dispositif contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements R et des réponses D,

• • les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent d' tel que

$$d' = h(\text{message}, R)$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{ mod } n$$

11. Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à un dispositif contrôleur,

- l'authenticité de l'entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen :

- de **m** couples de valeurs privées **Q₁, Q₂, ... Q_m** et publiques **G₁, G₂, ... G_m**, **m** étant supérieur ou égal à 1, ou des paramètres dérivés de ceux-ci,
- d'un module public **n** constitué par le produit de **f** facteurs premiers **P₁, P₂, ... P_f**, **f** étant supérieur ou égal à 2 ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{ mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n ;$$

v désignant un exposant public tel que :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique **G_i** étant le carré **g_i²** d'un nombre de base **g_i** inférieur aux **f** facteurs premiers **p₁, p₂, ... p_f** ; le nombre de base **g_i** étant tel que les conditions suivantes sont satisfaites:

aucune des deux équations :

$$x^2 \equiv g_i \text{ mod } n \quad \text{et} \quad x^2 \equiv -g_i \text{ mod } n$$

n'a de solution en **x** dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n ;

ledit dispositif terminal comprend un dispositif témoin comportant,

- une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public v ;

ledit dispositif témoin comporte aussi

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,,
10

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

ou r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;
20
ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ;
25
chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots \cdot Q_m^{dm} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \dots \cdot Q_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

12. Dispositif terminal selon la revendication 11 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

5 le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• **étapes 2 et 3 : acte de défi **d**, acte de réponse **D****

10 les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin, les moyens de calcul des réponses **D** du dispositif témoin, calculent les
15 réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle,

20 **13. Dispositif terminal selon la revendication 11 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,**
ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant
25 interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,
ledit dispositif démonstrateur comportant des moyens de connexion pour le

connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur,

ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**,

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

5 les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

14. Dispositif terminal selon la revendication 11 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;

10 le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

15 ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

20 ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

25

Opération de signature

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement **R****

à chaque appel, les moyens de calcul des engagements **R** du dispositif

témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

• étape 2 : acte de défi **d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• étape 3 : acte de réponse **D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

15. Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur, destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen :

- de **m** couples de valeurs publiques **G₁, G₂, ... G_m**, **m** étant supérieur ou égal à 1,

- d'un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f , f étant supérieur ou égal à 2, inconnus du dispositif contrôleur et de l'entité contrôleur associé ;

ledit module et lesdites valeurs étant liés par des relations du type :

5

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n} ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i ,

v désignant un exposant public tel que

$$v = 2^k$$

10

où k est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_1, p_2, \dots, p_f ; le nombre de base g_i étant tel que les conditions suivantes sont satisfaites :

aucune des deux équations :

15

$$x^2 \equiv g_i \pmod{n} \quad \text{et} \quad x^2 \equiv -g_i \pmod{n}$$

n'a de solution en x dans l'anneau des entiers modulo n

l'équation :

$$x^v \equiv g_i^2 \pmod{n}$$

a des solutions en x dans l'anneau des entiers modulo n ;

20

16. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

25

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- étapes 1 et 2 : acte d'engagement R , acte de défi d

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers **d_i** ci-après appelés défis élémentaires,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \text{mod } n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu,

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 5972.WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR99/02524	International filing date (day/month/year) 15 October 1999 (15.10.99)	Priority date (day/month/year) 15 October 1998 (15.10.98)
International Patent Classification (IPC) or national classification and IPC G06T 17/20		
Applicant FRANCE TELECOM		

COPIE

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.



This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 15 May 2000 (15.05.00)	Date of completion of this report 20 November 2000 (20.11.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/02524

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

- ☐ the international application as originally filed.
- ☒ the description, pages 1-38, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. 1-23, filed with the letter of 20 October 2000 (20.10.2000),
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/12, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-23	YES
	Claims		NO
Inventive step (IS)	Claims	1-23	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-23	YES
	Claims		NO

2. Citations and explanations

The available prior art does not disclose or suggest a method which takes into account the number of edges at each vertex to optimise the position of the resulting vertex, as defined in Claim 1. For this reason, Claims 1-23 meet the requirements of PCT Article 33(2) and (3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Contrary to the requirements of PCT Rule 5.1(a)(ii), the description does not outline the relevant prior art set forth in document D1 (US-A-5 590 248) and does not cite this document.

PCTORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ :**H04L 9/32****A2**

(11) Numéro de publication internationale:

WO 00/45550

(43) Date de publication internationale:

3 août 2000 (03.08.00)

(21) Numéro de la demande internationale: **PCT/FR00/00190**(22) Date de dépôt international: **27 janvier 2000 (27.01.00)**

(30) Données relatives à la priorité:

99/01065	27 janvier 1999 (27.01.99)	FR
99/03770	23 mars 1999 (23.03.99)	FR
99/12465	1er octobre 1999 (01.10.99)	FR
99/12467	1er octobre 1999 (01.10.99)	FR
99/12468	1er octobre 1999 (01.10.99)	FR

(71) Déposants (pour tous les Etats désignés sauf US): **FRANCE**
TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris
(FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue
d'Oradour-sur-Glane, F-75732 Paris cedex 15 (FR). MATH
RIZK [BE/BE]; Verte Voie, 20 Boîte 5, B-1348 Lou-
vain-la-Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants (US seulement): **GUILLOU, Louis**
[FR/FR]; 16, rue de l'Ise, F-35230 Bourgarre (FR).
QUISQUATER, Jean-Jacques [BE/BE]; 3, avenue des
Canards, B-1640 Rhode Saint Genese (BE).(74) Mandataire: **VIDON, Patrice; Cabinet Patrice Vidon, Im-**
meuble Germanium, 80, avenue des Buttes de Coësmes,
F-35700 Rennes (FR).(81) Etats désignés: **AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR,**
BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD,
SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US,
UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS,
MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ,
BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE,
CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

*Sans rapport de recherche internationale, sera republiée dès
réception de ce rapport.***COPIE**(54) Title: **METHOD FOR PROVING THE AUTHENTICITY OR INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC
EXPONENT EQUAL TO THE POWER OF TWO**(54) Titre: **PROCEDE DESTINE A PROUVER L'AUTHEENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN MESSAGE AU MOYEN
D'UN EXPOSANT PUBLIC EGAL A UNE PUISSANCE DE DEUX**

(57) Abstract

Proof is established by means of the following parameters: m pairs of private values Q_i and public values G_i , $m > 1$, a public module n made of the product of f first factors p_j , $f > 2$, a public exponent v , linked to each other by relations of the type: $G_i \cdot Q_i^v = 1 \pmod n$ or $G_i = Q_i^v \pmod n$. Said exponent v is such that $v = 2^k$ where $k > 1$ is a security parameter. Public value G_i is the square g_i^2 of a base number g_i that is lower than f first factors p_j , so that the two equations: $x^2 = g_i \pmod n$ and $x^2 = -g_i \pmod n$ do not have a solution in x in the ring of the modulo n integers and such that the equation $x^v = g_i^2 \pmod n$ has solutions in x in the ring of the modulus n integers.

(57) Abrégé

La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques G_i , $m > 1$; un module public n constitué par le produit de f facteurs premiers p_j , $f > 2$, un exposant public v , liés par des relations du type: $G_i \cdot Q_i^v = 1 \pmod n$ ou $G_i = Q_i^v \pmod n$. Ledit exposant v est tel que $v = 2^k$ où $k > 1$ est un paramètre de sécurité. Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_j , tel que les deux équations: $x^2 = g_i \pmod n$ et $x^2 = -g_i \pmod n$ n'ont pas de solution en x dans l'anneau des entiers modulo n , et tel que l'équation $x^v = g_i^2 \pmod n$ a des solutions en x dans l'anneau des entiers modulo n .

**Method, system and device for proving the authenticity of an entity
and/or the integrity and/or the authenticity of a message using specific
prime factors**

5 The present invention relates to the technical field of methods,
systems and devices designed to prove the authenticity of an entity and/or
the integrity and/or authenticity of a message.

10 The patent EP 0 311 470 B1, whose inventors are Louis Guillou and
Jean-Jacques Quisquater, describes such a method. Hereinafter, reference
shall be made to their work by the terms "GQ patent" or "GQ method".
Hereinafter, the expression "GQ2", or "GQ2 invention" or "GQ2
technology" shall be used to describe the new developments of the GQ
technology that are the object of pending applications filed on the same
day as the present application by France Telecom, TDF and the firm
Mathrizk, and having Louis Guillou and Jean-Jacques Quisquater as their
15 inventors. The characteristic features of these pending applications are
recalled whenever necessary in the following description.

20 According to the GQ method, an entity known as a "trusted
authority" assigns an identity to each entity called a "witness" and
computes its RSA signature. In a customizing process, the trusted
authority gives the witness an identity and signature. Thereafter, the
witness declares the following: "Here is my identity; I knew the RSA
signature thereof". The witness, without revealing the fact, proves that he
knows the RSA signature of his identity. Through the RSA public
identification key distributed by the trusted authority, an entity known as
25 a "controller" ascertains, without obtaining knowledge thereof, that the
RSA signature corresponds to the declared identity. The mechanism using
the GQ method takes place "without transfer of knowledge". According to
the GQ method, the witness does not know the RSA private key with
which the trusted authority signs a large number of identities.

The GQ technology described here above makes use of RSA technology. However, while the RSA technology truly depends on the factorization of the modulus n , this dependence is not an equivalence, indeed far from it, as can be seen in the so-called multiplicative attacks against various standards of digital signatures implementing the RSA technology.

The goal of the GQ2 technology is twofold: firstly to improve the performance characteristics of RSA technology and secondly to avert the problems inherent in RSA technology. Knowledge of the GQ2 private key is equivalent to knowledge of the factorization of the modulus n . Any attack on the triplets GQ2 leads to the factorization of the modulus n : this time there is equivalence. With the GQ2 technology, the work load is reduced for the signing or self-authenticating entity and for the controlling entity. Through a better use of the problem of factorizing in terms of both security and performance, the GQ2 technology averts the drawbacks of RSA technology.

The GQ method implements modulo computations of numbers comprising 512 bits or more. These computations relate to numbers having substantially the same size raised to powers of the order of $2^{16} + 1$. Now, existing microelectronic infrastructures, especially in the field of bank cards, make use of monolithic self-programmable microprocessors without arithmetical coprocessors. The work load related to multiple arithmetical applications involved in methods such as the GQ method leads to computation times which, in certain cases, prove to be disadvantageous for consumers using bank cards to pay for their purchases. It may be recalled here that, in seeking to increase the security of payment cards, the banking authorities have raised a problem that is particularly difficult to resolve. Indeed, two apparently contradictory questions have to be resolved: on the one hand, increasing safety by using increasingly lengthy and distinct

keys for each card while, on the other hand, preventing the work load from leading to excessive computation times for the user. This problem becomes especially acute inasmuch as it is also necessary to take account of the existing infrastructure and the existing microprocessor components.

5 The GQ2 technology provides a solution to this problem while boosting security.

The GQ2 technology implements prime factors having special properties. There are various existing techniques for producing these prime factors. An object of the present invention is a method for the systematic production of such prime factors. It also relates to the application that can be made of these factors especially in the implementation of the GQ2 technology. It must be emphasized right now that these special prime factors and the method used to obtain them can be applied beyond the field of GQ2 technology.

15 The invention can be applied to a method (GQ2 method) designed to prove the following to a controller entity:

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives thereof:

- a public modulus n constituted by the product of f prime factors p_1, p_2, \dots, p_f (f being equal to or greater than 2),
- a public exponent v ;
- m distinct integer base numbers g_1, g_2, \dots, g_m (m being greater than or equal to 1).

25 The base numbers g_i are such that the two equations (1) and (2):

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

cannot be resolved in x in a ring of integers modulo n , and such that the equation (3):

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of integers modulo n .

The method according to the invention is used to produce the f prime factors p_1, p_2, \dots, p_f in such a way that the equations (1), (2) and (3) are satisfied. The method according to the invention comprises the step of choosing firstly:

- the m base numbers g_1, g_2, \dots, g_m ,
- the size of the modulus n ,
- the size of the f prime factors p_1, p_2, \dots, p_f .

The method relates to the case where the public exponent v has the form:

$$v = 2^k$$

where k is a security parameter greater than 1. The security parameter k is also chosen as a prime number. This special value of the exponent v is one of the essential features of GQ2 technology.

Preferably, the m base numbers g_1, g_2, \dots, g_m , are chosen at least partially among the first integers. Preferably again, the security parameter k is a small integer, especially below 100. Advantageously, the size of the modulus n is greater than several hundreds of bits. Advantageously again, the f prime factors p_1, p_2, \dots, p_f have a size close to the size of the modulus n divided by the number f of factors.

According to a major characteristic of the method according to the invention, the f prime factors p_1, p_2, \dots, p_f are not chosen in any unspecified way. Among the f prime factors p_1, p_2, \dots, p_f , a certain number of them: e will be chosen to be congruent to 1 modulo 4. This number e of prime factors may be zero. Should e be zero, the modulus n will hereinafter be called a basic modulus. Should $e > 0$, the modulus n will hereinafter be called a combined modulus. The $f-e$ other prime factors are chosen to be congruent to 3 modulo 4. This number $f-e$ of prime factors is at least equal

to 2.

Choice of f-e prime factors congruent to 3 modulo 4

To produce the f-e prime factors p_1, p_2, \dots, p_{f-e} congruent to 3 modulo 4, the following steps are implemented:

- 5 - the first prime factor p_1 congruent to 3 modulo 4 is chosen and then,
- the second prime factor p_2 is chosen such that p_2 is complementary to p_1 with respect to the base number g_1 .

To choose the factor p_{i+1} , the following procedure is used in distinguishing two cases:

- 10 (1) the case where $i > m$

Should $i > m$, the factor p_{i+1} congruent to 3 modulo 4 is chosen.

- (2) Case where $i \leq m$

Should $i \leq m$, the Profile ($\text{Profile}_i(g_i)$) of g_i with respect to i first prime factors p_i is computed:

- 15 • if the $\text{Profile}_i(g_i)$ is flat, the factor p_{i+1} is chosen such that p_{i+1} is complementary to p_i with respect to g_i ,

 • else, among the $i-1$ base numbers g_1, g_2, \dots, g_{i-1} and all their multiplicative combinations, the number, hereinafter called g is chosen such that $\text{Profile}_i(g) = \text{Profile}_i(g_i)$, and then p_{i+1} is chosen such that

20 $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$.

The terms “complementary”, “profile”, “flat profile” have the meanings defined in the description.

To choose the last prime factor p_{f-e} , the following procedure is used in distinguishing three cases:

- 25 (1) Case where $f-e-1 > m$

Should $f-e-1 > m$, p_{f-e} is chosen congruent to 3 modulo 4.

- (2) Case where $f-e-1 = m$

Should $f-e-1 = m$, $\text{Profile}_{f-e-1}(g_m)$ is computed with respect to $f-e-1$ first prime factors from p_1 to p_{f-e-1} ,

- if $\text{Profile}_{f-e-1}(g_m)$ is flat, p_{f-e-1} is chosen such that it is complementary to p_1 with respect to g_m ,

- else, the procedure stipulated here below is followed:

Among the $m-1$ base numbers from g_1 to g_{m-1} and all their multiplicative combinations, the number hereinafter called g is chosen such that $\text{Profile}_1(g) = \text{Profile}_1(g_1)$ and then p_{f-e} is chosen such that $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$.

(3) Case where $f-e-1 < m$

If $f-e-1 < m$, then p_{f-e} is chosen such that the following two conditions are met:

(3.1) First condition

$\text{Profile}_{f-e-1}(g_{f-e-1})$ is computed with respect to the $f-e-1$ first prime factors from p_1 to p_{f-e-1} . Two cases are then to be considered. Depending on either of these two cases, the first condition will be different.

If $\text{Profile}_{f-e-1}(g_{f-e-1})$ is flat, p_{f-e} is chosen so that it meets the first condition of being complementary to p_1 with respect to g_{f-e-1} (first condition according to the first case). Else, among the $f-e-1$ base numbers from g_1 to g_{m-1} and all their multiplicative combinations, the number, hereinafter called g , is chosen such that $\text{Profile}_1(g) = \text{Profile}_{f-e-1}(g_{f-e-1})$ and then p_{f-e} is chosen so that it meets the condition of being such that $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$, (first condition according to the second case).

(3.2) Second condition

Among all the last base numbers from g_{f-e} to g_m , those numbers whose Profile $\text{Profile}_{f-e-1}(g_i)$ is flat are chosen and then p_{f-e} is chosen so that it meets the condition of being complementary to p_1 with respect to each of the base numbers thus selected (second condition).

Choice of e prime factors congruent to 1 modulo 4

To produce the e prime factors congruent to 1 modulo 4, each prime

factor candidate p is evaluated, from p_{t-2} to p_t in being subjected to the following two successive tests:

(1) First test

The Legendre symbol is computed for each base number g_i , from g_1 to g_m , with respect to the candidate prime factor p ,

- if the Legendre symbol is equal to -1 , the candidate p is rejected,
- if the Legendre symbol is equal to $+1$, the evaluation of the candidate p is continued in passing to the following base number and then, when the last base number has been taken into account, there is a passage to the second test.

(2) Second test

An integer number t is computed such that $p-1$ is divisible by 2^t , but not by 2^{t+1} , then an integer s is computed such that $s = (p-1+2^t)/2^{t+1}$.

The key $\langle s, p \rangle$ is applied to each public value G_i to obtain a result r

$$r \equiv G_i^s \pmod{p}$$

If r is equal to g_i or $-g_i$, the second test is continued in passing to the following public value G_{i+1} .

If r is different from g_i or $-g_i$, a factor u is computed in applying the following algorithm specified for an index ii ranging from 1 to $t-2$. The algorithm implements two variables: w initialized by r and $jj = 2^{ii}$ assuming values ranging from 2 to 2^{t-2} , as well a number b obtained by application of the key $\langle (p-1)/2^t, p \rangle$ to a non-quadratic residue of $CG(p)$. The algorithm consists in repeating the following sequence as many times as is necessary:

- Step 1: $w^2/G_i \pmod{p}$ is computed,
- Step 2: the result is raised to the power of 2^{t-ii-1} . Two cases are to be considered.

First case

If $+1$ is obtained, there is a passage to the following public value G_{i+1} and the second test is performed for this public value.

Second case

If -1 is obtained, $jj = 2^{ii}$ is computed and then w is replaced by $w.b^{jj} \pmod{p}$. Then, the algorithm is continued for the following value having an index ii .

At the end of the algorithm, the value in the variable jj is used to compute an integer u by the relation $jj = 2^{t-u}$ and then the expression $t-u$ is computed. Two cases arise:

- if $t-u < k$, the candidate p is rejected
- if $t-u > k$, the evaluation of the candidate p is continued in passing to the following public value G_{i+1} and then in continuing the second test.

The candidate p is accepted as a prime factor congruent to 1 modulo 4 if, at the end of the second test, for all the m public values G_i , it has not been rejected.

Application to the public and private values of GQ2

The present invention also relates to a method (GQ2 method) applying the method that has just been described and making it possible, it may be recalled, to produce f prime factors p_1, p_2, \dots, p_f having special properties; The method for the application of the method that has just been described is designed to prove the following to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),
- the public modulus n constituted by the product of said prime factors $f p_1, p_2, \dots, p_f$ (f being greater than or equal to 2),
- the public exponent v .

Said modulus, said exponent and said values are linked by relations

of the following type:

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

Said exponent v is such that

$$v = 2^k$$

5 where k is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of the base number g_i smaller than the f prime factors p_1, p_2, \dots, p_f . The base number g_i is such that the two equations:

$$x^2 \equiv g_i \pmod{n} \quad \text{and} \quad x^2 \equiv -g_i \pmod{n}$$

10 cannot be resolved in x in the ring of integers modulo n and such that the equation:

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of the integers modulo n .

15 Said method implements an entity called a witness in the following steps. Said witness entity has f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or of the public modulus n and/or the m private values Q_i and/or $f \cdot m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent v .

20 The witness computes commitments R in the ring of integers modulo n . Each commitment is computed:

- either by performing operations of the type:

$$R \equiv r^v \pmod{n}$$

where r is a random factor such that $0 < r < n$,

- or by performing operations of the type:

25
$$R_i \equiv r_i^v \pmod{p_i}$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random factors $\{r_1, r_2, \dots, r_f\}$, then by applying the Chinese remainder method.

The witness receives one or more challenges d . Each challenge d

comprises m integers d_i hereinafter called elementary challenges. The witness, on the basis of each challenge d_i , computes a response D_i ,

- either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \pmod{n}$$

- or by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \pmod{p_i}$$

and then by applying the Chinese remainder method.

The method is such that there are as many responses D as there are challenges d as there are commitments R , each group of numbers R, d, D forming a triplet referenced $\{R, d, D\}$.

Preferably, in order to implement the pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m as just described, the method uses the prime factors p_1, p_2, \dots, p_f and/or the parameters of the Chinese remainders, the base numbers g_1, g_2, \dots, g_m and/or the public values G_1, G_2, \dots, G_m to compute:

- either the private values Q_1, Q_2, \dots, Q_m by extracting a k -th square root modulo n of G_i , or by taking the inverse of a k -th square root modulo n of G_i ,

- or the $f \cdot m$ private components $Q_{i,j}$ of the private values Q_1, Q_2, \dots, Q_m such that $Q_{i,j} \equiv Q_i \pmod{p_j}$.

More particularly, to compute the $f \cdot m$ private components $Q_{i,j}$ of the private values Q_1, Q_2, \dots, Q_m :

- the key $\langle s, p_j \rangle$ is applied to compute z such that:

$$z \equiv G_i^s \pmod{p_j}$$

- and the values t and u are used.

The values t and u are computed as indicated here above when p_j is congruent to 1 modulo 4. The values t and u are taken to be respectively equal to 1 ($t=1$) and 0 ($u=0$) where p_j is congruent to 3 modulo 4.

If the value u is zero, we consider all the numbers zz such that:

• • • zz is equal to z or such that

• • • zz is equal to a product (mod p_j) of z by each of the 2^{ii-t} 2^{ii} -th primitive roots of unity, ii ranging from 1 to $\min(k,t)$.

If u is positive, we can consider all the numbers zz such that zz is equal to the product (mod p_j) of za by each of the 2^k 2^k -th roots of unity, za designating the value of the variable w at the end of the algorithm described here above.

At least one value of the component $Q_{t,j}$ is deduced therefrom. It is equal to zz when the equation $G_i \equiv Q_i^v \pmod{n}$ is used or else it is equal to the inverse of zz modulo p_j of zz when the equation $G_i \cdot Q_i^v \equiv 1 \pmod{n}$ is used.

Description

The goal of GQ technology may be recalled: it is the dynamic authentication of entities and associated messages as well as the digital signature of messages.

5 The standard version of GQ technology makes use of RSA technology. However, although the RSA technology truly depends on factorizing, this dependence is not an equivalence, far from it, as can be shown from attacks, known as multiplicative attacks, against various digital signature standards implementing RSA technology.

10 In the context of GQ2 technology, the present part of the invention relates more specifically to the production of sets of GQ2 keys designed to provide for dynamic authentication and digital signature. The GQ2 technology does not use RSA technology. The goal is a twofold one: firstly to improve performance with respect to RSA technology and
15 secondly to prevent problems inherent in RSA technology. The GQ2 private key is the factorization of the modulus n . Any attack on the GQ2 triplets amounts to the factorizing of the modulus n : this time there is equivalence. With the GQ2 technology, the work load is reduced both for the entity that signs or is authenticated and for the one that controls.
20 Through an improved use of the problem of factorization, in terms of both security and performance, the GQ2 technology rivals the RSA technology.

25 The GQ2 technology uses one or more small integers greater than 1, for example m small integers ($m \geq 1$) called base numbers and referenced g_i . Then, a public verification key $\langle v, n \rangle$ is chosen as follows. The public verification exponent v is 2^k where k is a small integer greater than 1. ($k \geq 2$). The public modulus n is the product of at least two prime factors greater than the base numbers, for example f prime factors ($f \geq 2$) referenced by p_j , from $p_1 \dots p_f$. The f prime factors are chosen so that the public modulus n has the following properties with respect to each of the

m base numbers from g_1 to g_m .

- Firstly, the equations (1) and (2) cannot be resolved in x in the ring of the integers modulo n , that is to say that g_i and $-g_i$ are two non-quadratic residues (mod n).

$$x^2 \equiv g_i \pmod{n} \quad (1)$$

$$x^2 \equiv -g_i \pmod{n} \quad (2)$$

- Secondly, the equation (3) can be resolved in x in the ring of the integers modulo n .

$$x^{2^k} \equiv g_i^2 \pmod{n} \quad (3)$$

Hereinafter, these properties are also called the GQ2 principles.

Since the public verification key $\langle v, n \rangle$ is fixed according to the base numbers from g_1 to g_m with $m \geq 1$, each base number g_i determines a pair of values GQ2 comprising a public value G_i and a private value Q_i : giving m pairs referenced $G_1 Q_1$ to $G_m Q_m$. The public value G_i is the square of the base number g_i : giving $G_i = g_i^2$. The private value Q_i is one of the solutions to the equation (3) or else the inverse (mod n) of such a solution.

Just as the modulus n is broken down into f prime factors, the ring of the integers modulo n are broken down into f Galois fields, from $CG(p_1)$ to $CG(p_f)$. Here are the projections of the equations (1), (2) and (3) in $CG(p_j)$.

$$x^2 \equiv g_i \pmod{p_j} \quad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \quad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \quad (3.a)$$

Each private value Q_i can be represented uniquely by f private components, one per prime factor: $Q_{ij} \equiv Q_i \pmod{p_j}$. Each private component Q_{ij} is a solution to the equation (3.a) or else the inverse (mod p_j) of such a solution. After all the possible solutions to each equation (3.a) have been computed, the Chinese remainder technique sets up all the possible values for each private value Q_i on the basis of f components of $Q_{i,1}$ to $Q_{i,f}$: $Q_i = \text{Chinese remainders}(Q_{i,1}, Q_{i,2}, \dots, Q_{i,f})$ so as to obtain all the

possible solutions to the equation (3).

The following is the Chinese remainder technique: let there be two positive integers that are mutually prime numbers a and b such that $0 < a < b$, and two components X_a from 0 to $a-1$ and X_b from 0 to $b-1$. It is required to determine $X = \text{Chinese remainders } (X_a, X_b)$, namely the single number X of 0 to $a.b-1$ such that $X_a \equiv X \pmod{a}$ and $X_b \equiv X \pmod{b}$. The following is the Chinese remainder parameter: $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. The following is the Chinese remainder operation: $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; if δ is negative, replace δ by $\delta + a$; $\gamma \equiv \alpha \cdot \delta \pmod{a}$; $X = \gamma \cdot b + X_b$.

When the prime factors are arranged in increasing order, from the smallest p_1 to the greater p_f , the Chinese remainder parameters can be the following (there are $f-1$, namely at least one of the prime factors). The first Chinese remainder parameter is $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. The second Chinese remainder parameter is $\beta \equiv \{p_1, p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. The i -th Chinese remainder parameter is $\lambda \equiv \{p_1, p_2, \dots, p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. And so on and so forth. Finally, in $f-1$ Chinese remainder operations, a first result $(\text{mod } p_2 \text{ times } p_1)$ is obtained with the first parameter and then a second result $(\text{mod } p_1, p_2 \text{ times } p_3)$ with the second parameter and so on and so forth until a result $(\text{mod } p_1, \dots, p_{f-1} \text{ time } p_f)$, namely $(\text{mod } n)$.

The object of the invention is a method for the random production of any set of GQ2 keys among all the sets possible, namely:

- the random production of any moduli among all the GQ2 moduli possible, namely the moduli ensuring that, for each of the m base numbers g_i , the equations (1) and (2) cannot be resolved in x in the ring of integers modulo n while the equation (3) has one of them,
- computing all the possible solutions to each of the equations (3.a). The Chinese remainder technique enables the obtaining of a private value Q_i from each set of f components from $Q_{i,1}$ to $Q_{i,f}$, so as to obtain any solution in x for the equation (3) among all the possible equations.

Q_i = Chinese remainders ($Q_{i,1}, Q_{i,2}, \dots, Q_{i,p}$)

To grasp the problem, and then understand the solution to be given to the problem, namely the invention, we shall first of all analyze the applicability of the principles of GQ2 technology. Let us start by recalling the notion of rank in a Galois field $CG(p)$ in order to study the functions "raised to the square in $CG(p)$ " and "take a square root of a quadratic residue in $CG(p)$ ". Then, we shall analyze the existence and number of solutions in x in $CG(p)$ to the equations (1.a), (2.a) and (3.a).

Rank of the elements in $CG(p)$

Let us take a odd prime number p and a positive prime number a smaller than p . Let us thereafter define $\{X\}$.

$$\{X\} \equiv \{x_1 = a; \text{ puis, pour } i \geq 1, x_{i+1} \equiv a.x_i \pmod{p}\}$$

Let us calculate the term for the index $i+p$ and let us use Fermat's theorem:

$$x_{i+p} \equiv a^p x_i \equiv a.x_i \equiv x_{i+1} \pmod{p}$$

Consequently, the period of the sequence $\{X\}$ is $p-1$ or a divider of $p-1$. This period depends on the value of a . By definition, this period is called "the rank of $a \pmod{p}$ ". It is the index of appearance of unity in the sequence $\{X\}$.

$$x_{rank(a,p)} \equiv 1 \pmod{p}$$

For example, when $(p-1)/2$ is an odd prime number p' , the Galois field $CG(p)$ comprises a single element with a rank 1: it is 1, a single element with rank 2. It is -1 , $p'-1$ elements of a rank p' , $p'-1$ elements of the rank $2.p'$, namely of the rank $p-1$.

The elements of $CG(p)$ whose rank is $p-1$ are called the primitive elements or again the generators of $CG(p)$. The name is due to the fact that their successive powers in $CG(p)$, namely the terms of the $\{X\}$ sequence for the indices going from 1 to $p-1$, form a permutation of all the non-zero elements of $CG(p)$.

According to a primitive element y of $CG(p)$, let us evaluate the rank

of the element $y^i \pmod{p}$ as a function of i and $p-1$. When i is a prime number with $p-1$, it is $p-1$. When i divides $p-1$, it is $(p-1)/i$. In all cases, it is $(p-1)/\text{pgcd}(p-1, i)$.

The Euler function is referenced by φ . By definition, since n is a positive integer, $\varphi(n)$ is the number of positive integers smaller than n that are prime numbers with n . In the field $\text{CG}(p)$, there are therefore $\varphi(p-1)$ primitive elements.

By way of an illustration, here is the base of the RSA technology. The public modulus n is the product of f prime factors from p_1 to p_f with $f \geq 2$, such that for each prime factor p_j , the public exponent v is a prime number with p_j-1 . The key $\langle v, p_j \rangle$ complies with the rank of the elements of $\text{CG}(p_j)$: it permutes them. The inverse permutation is obtained with a key $\langle s_j, p_j \rangle$ such that p_j-1 divides $v \cdot s_j - 1$.

Squares and square roots in $\text{CG}(p)$

The elements x and $p-x$ have the same square in $\text{CG}(p)$. The key $\langle 2, p \rangle$ do not permute the elements of $\text{CG}(p)$ because $p-1$ is an even value. For each prime number p , let us define an integer t as follows: $p-1$ is divisible by 2^t , but not by 2^{t+1} , namely p is congruent to $2^t+1 \pmod{2^{t+1}}$. For example $t=1$ when p is congruent to 3 (mod 4); $t=2$ when p is congruent to 5 (mod 8); $t=3$ when p is congruent to 9 (mod 16); $t=4$ when p is congruent to 17 (mod 32); and so on and so forth. Each odd prime number is seen in one and only one category: p is seen in the t -th category. In practice, if we consider a fairly large number of successive prime numbers, about one in every two is found in the first category, one in four in the second, one in eight in the third, one in sixteen in the fourth, and so on and so forth. In short, one in 2^t on an average is found in the t -th category.

Let us consider the behavior of the function "raise to the square in $\text{CG}(p)$ " according to the parity of the rank of the argument.

- There is only one fixed element: it is 1. The square of any other element of an odd-parity rank is another element having the same rank. Consequently, the key $\langle 2, p \rangle$ permutes all its $(p-1)/2'$ odd-parity rank elements. The number of permutation cycles depends on the factorization of $(p-1)/2'$. For example, when $(p-1)/2'$ is a prime number p' , there is a big permutation cycle comprising $p'-1$ elements.
- The square of any even-parity rank element is another element whose rank is divided by two. Consequently, the even-parity ranking elements are distributed over $(p-1)/2'$ branches. Each non-zero element with an odd-parity rank bears a branch with a length t comprising 2^t-1 elements, namely: an element of a rank divisible by two but not by four and then, if $t \geq 2$, two elements of a rank divisible by four but not by eight, and then if $t \geq 3$, four elements of a rank divisible by eight but not by sixteen, and then if $t \geq 4$, eight elements of a rank divisible by sixteen but not by 32 and so on and so forth. The 2^{t-1} ends of each branch are non-quadratic residues; their rank is divisible by 2^t .

Figures 1A to 1D illustrate the function "raise to the square in $CG(p)$ " by an oriented graph where each of the $p-1$ non-zero elements of the field finds its place: the non-quadratic residues are in white and the quadratic residues are in black; among the quadratic residues, the odd-parity ranking elements are in circles.

These figures show respectively;

- Figure 1A: the case where p is congruent to 3 (mod 4);
- Figure 1B: the case where p is congruent to 5 (mod 8);
- Figure 1C: the case where p is congruent to 9 (mod 16);
- Figure 1D: the case where p is congruent to 17 (mod 32).

Let us now look at the way to calculate a solution in x to the equation $x^2 \equiv a \pmod{p}$, it being known that a is a quadratic residue of

CG(p), namely how "to take a square root in CG(p)". There are of course several ways of obtaining the same result: the reader can advantageously consult Henri Cohen, *"A Course in Computational Algebraic Number Theory"*, published, Springer, Berlin, 1993, pp. 31-36 as well as *"Graduate Texts in Mathematics"*, vol. 138 (GTM 138).

Let us calculate an integer $s = (p-1+2^t)/2^{t+1}$ to establish a key $\langle s, p \rangle$. Let: $\langle (p+1)/4, p \rangle$ when p is congruent to 3 (mod 4), $\langle (p+3)/8, p \rangle$ when p is congruent to 5 (mod 8), $\langle (p+7)/16, p \rangle$ when p is congruent to 9 (mod 16), $\langle (p+15)/32, p \rangle$ when p is congruent to 17 (mod 32), and so and so forth.

- The key $\langle s, p \rangle$ gives the odd-parity ranking square root of any odd-parity ranking element. Indeed, in CG(p), r^2/a is equal to a raised to the power $(2 \cdot (p-1+2^t)/2^{t+1}) - 1 = (p-1)/2^t$. Consequently, when a is in a cycle, the key $\langle s, p \rangle$ converts a into a solution that we shall call w . The other solution is $p-w$.
- In general, the key $\langle s, p \rangle$ converts any quadratic residue a into a first approximation of a solution which shall be called r . The following are two key points followed by a rough sketch of a method for the step-by-step improvement of the approximation up to a square root of a .
 - Firstly, since a is a quadratic residue, the key $\langle 2^{t-1}, p \rangle$ certainly converts r^2/a into 1.
 - Secondly, it may be assumed that we know a non-quadratic residue of CG(p) that we name y ; the key $\langle (p-1)/2^t, p \rangle$ converts y into an element that shall be called b : this is a root 2^{t-1} -th of -1 . Indeed, $y^{(p-1)/2} \equiv -1 \pmod{p}$. Consequently, in CG(p), the multiplicative group of the 2^t 2^t -th roots of unity is isomorphic to the multiplicative group of the powers of b for the exponents from 1 to 2^t .
 - To approach a square root of a , let us raise r^2/a to the power of $2^{t-2} \pmod{p}$: the result is $+1$ or -1 . The new approximation remains r if

the result is +1 or else it becomes $b.r \pmod{p}$ if the result is -1. Consequently, the key $\langle 2^{t-2}, p \rangle$ certainly converts the new approximation into 1. It is possible to continue to approach the required value: at the next step, an adjustment will be made if necessary by multiplying by $b^2 \pmod{p}$ and so on and so forth.

The following algorithm makes successive approximations to reach a square root of a from the integers r and b defined here above; it uses two integer variables: w initialized by r to represent the successive approximations and jj assuming values among the powers of 2, from 2 to 2^{t-2} .

For i ranging from 1 to $t-2$, repeat the following sequence:

- Compute $w^2/a \pmod{p}$, then raise the result to the power $2^{t-i-1} \pmod{p}$: +1 or -1 should be obtained. When -1 is obtained, compute $jj = 2^i$, then replace w by $w.b^{jj} \pmod{p}$. When +1 is obtained, do nothing.

At the end of the computation, w and $p-w$ are two square roots of a in $\text{CG}(p)$. Furthermore, we learn that the rank of a in $\text{CG}(p)$ is divisible by $2^t/jj$ but not by $2^{t+1}/jj$. The relevance of this observation will be seen further below.

Analysis of the principles of GQ2 technology in $\text{CG}(p)$

Let us take two integers g and k greater than 1 and a prime number p greater than g . Let us analyze the existence and number of solutions in x in $\text{CG}(p)$ in the equations (1.a), (2.a) and (3.a).

In the Galois field $\text{CG}(p)$, let us distinguish different cases depending on the value of t , namely, according to the power of two which divides $p-1$. It may be recalled that $p-1$ is divisible by 2^t , but not by 2^{t+1} , namely, that p is congruent to $2^t+1 \pmod{2^{t+1}}$. The previous analysis gives us a fairly precise idea of the problem raised as well as a rough solution.

When $t = 1$, p is congruent to 3 $\pmod{4}$. The Legendre symbols of g and $-g$ with respect to p are different: any quadratic residue of $\text{CG}(p)$ has

two square roots in $CG(p)$: one is a quadratic residue and the other is a non-quadratic residue. Firstly, one of the two equations (1.a) or (2.a) has two solutions in x in $CG(p)$ and the other does not have any. Secondly, the equation (3.a) has two solutions in x in $CG(p)$ whatever the value of k .

5 When $t = 2$, p is congruent to 5 (mod 8). Two cases occur, depending on the Legendre symbol of g with respect to p . When the symbol is equal to -1 , g and $-g$ are both non-quadratic residues of $CG(p)$: the three equations (1.a), (2.a) and (3.a) have no solution in x in $CG(p)$. When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of
10 $CG(p)$, each equation (1.a) and (2.a) has two solutions in x in $CG(p)$. Furthermore, the rank of g^2 in $CG(p)$ is an odd-parity value implying that whatever the value of k , the equation (3.a) has four solutions in x in $CG(p)$ of which only one has an odd-parity rank.

15 Figure 2 illustrates the solutions to the equation (3.a) with $k = 6$ and p congruent to 5 (mod 8), giving $t = 2$. It may be noted that, because the Legendre symbol of 2 with respect to p congruent to 5 (mod 8) is equal to $-1.2^{(p-1)/4} \pmod{p}$ is then a square root of -1 . We therefore have:

$$p \equiv 5 \pmod{8}; \text{ consequently } (2|p) = -1$$

$$p \equiv 2^{\frac{p-1}{4}} \pmod{p}; \text{ hence } b^2 \equiv -1 \pmod{p}$$

20 When $t = 3$, p is congruent to 9 (mod 16). Let us consider the Legendre symbol of g with respect to p . When the symbol is equal to -1 , g and $-g$ are two non-quadratic residues of $CG(p)$: the three equations (1.a), (2.a) and (3.a) have no solution in x in $CG(p)$. When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of $CG(p)$; each equation (1.a) and
25 (2.a) has two solutions in x in $CG(p)$. The existence of solutions in x to the equation (3.a) depends on the rank of g^2 in $CG(p)$. This rank is an odd-parity value or is divisible by two but not by four. When the rank of g^2 in $CG(p)$ is divisible by two but not by four, the equation (3.a) has four solutions in x in $CG(p)$ for $k = 2$; it cannot go above $k \geq 3$. When the rank

of g^2 in $CG(p)$ is an odd-parity value, the equation (3.a) has four solutions in x in $CG(p)$ for $k = 2$ and eight for $k \geq 3$. In both cases, only one value is an odd-parity value.

When $t = 4$, p is congruent to 17 (mod 32). Let us consider the Legendre symbol of g with respect to p . When the symbol is equal to -1 , g and $-g$ are two non-quadratic residues of $CG(p)$: the three equations (1.a), (2.a) and (3.a) have no solution in x in $CG(p)$. When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of $CG(p)$; each equation (1.a) and (2.a) has two solutions in x in $CG(p)$. The existence of solutions in x to the equation (3.a) depends on the rank of g^2 in $CG(p)$. This rank is an odd-parity value or is divisible by two or four but not by eight. When the rank of g^2 in $CG(p)$ is divisible by two but not by eight, the equation (3.a) has four solutions in x in $CG(p)$ for $k = 2$; it cannot go above $k \geq 3$. When the rank of g^2 in $CG(p)$ is divisible by two but not by four, the equation (3.a) has four solutions in x in $CG(p)$ for $k = 2$ or eight for $k = 3$; it has no solutions for $k \geq 4$. When the rank of g^2 in $CG(p)$ is an odd-parity value, the equation (3.a) has four solutions in x in $CG(p)$ for $k = 2$ and eight for $k \geq 3$ and sixteen for $k \geq 4$. In all three cases, only one value is an odd-parity value.

And so on and so forth so that the case where p is congruent to 1 (mod 4) can be summarized as follows.

When p is congruent to 1 (mod 4), let us consider the Legendre symbol of g with respect to p . When the symbol is equal to -1 , g and $-g$ are two non-quadratic residues of $CG(p)$: the three equations (1.a), (2.a) and (3.a) have no solution in x in $CG(p)$. When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of $CG(p)$; each equation (1.a) and (2.a) has two solutions in x in $CG(p)$. Let us define the integer u : the rank of g^2 in $CG(p)$ is divisible by 2^u , but not by 2^{u+1} . The value of u is among the $t-1$ possible values, from 0 to $t-2$. The existence and the number of solutions

in x in $CG(p)$ to the equation (3.a) depend on the values of k , t and u . When u is positive and k is greater than $t-u$, the equation (3.a) does not have a solution in x in $CG(p)$. When u is zero and k is greater than t , the equation (3.a) has 2^t solutions in x in $CG(p)$. When k is smaller than or equal to $t-u$, the equation (3.a) has 2^k solutions in x in $CG(p)$.

Applicability of the GQ2 principles in the rings of integers modulo

In order that the equation (1) and (2) respectively may have no solution in x in the ring of the integers modulo n , it is necessary and sufficient that, for at least one of the prime factors p , from p_1 to p_r , the equation (1.a) and (2.a) respectively will have no solution in x in $CG(p)$.

In order that the equation (3) may have solutions in x in the ring of the integers modulo n , it is necessary and sufficient that, for each of the prime factors p , from p_1 to p_r , the equation (3.a) should have solutions in x in $CG(p)$.

The equation (3) prohibits any prime factor p congruent with 1 (mod 4) as soon as, for one of the base numbers g , from g_1 to g_m : either the Legendre symbol of g with respect to p is equal to -1 ; or else the Legendre symbol of g with respect to p is equal to $+1$ with the condition: u positive and greater than $t-k$. In order that a prime factor p congruent to 1 (mod 4) may be possible, it is necessary to fulfill one of the following two conditions for each of the base numbers g , from g_1 to g_m , according to the two integers t and u defined here above. Either the rank of $G = g^2$ is an odd-parity rank in $CG(p)$, namely $u = 0$, whatever the value of k . Or else the rank of $G = g^2$ is an even-parity rank value in $CG(p)$, namely $u > 0$ and it meets the condition: $u + k \leq t$.

A product of prime factors congruent to 1 (mod 4) cannot fulfill all the principles of GQ2 technology. Each GQ2 modulus must have at least two prime factors congruent to 3 (mod 4) such that, for each base number

g , the Legendre symbol of g with respect to one of these factors differs from the Legendre symbol of g with respect to the other. When all the prime factors are congruent to 3 (mod 4), it will be said that the **GQ2 modulus is basic**. When, in addition to at least two prime factors congruent to 3 (mod 4), the modulus includes one or more prime factors congruent to 1 (mod 4), it will be said that the **modulus GQ2 is combined**.

Systematic construction of moduli GQ2

At the outset, it is necessary to fix the total constraints to be dictated on the modulus n : a size expressed in bits (for example, 512 or 1024 bits) as well as a number of most significant successive bits at 1 (at least one of course typically 16 or 32 bits), a number f of prime factors and a number e (possibly zero) of prime factors having to be congruent to 1 (mod 4); the other prime factors, namely $f-e$ factors, at least two, must be congruent to 3 (mod 4). The modulus n will be the product of f prime factors of similar sizes. When $e = 0$, a basic modulus GQ2 is obtained; when $e > 0$, a combined modulus GQ2 is obtained. A basic modulus is the product of prime factors all congruent to 3 (mod 4). A combined modulus GQ2 appears therefore as the product of a basic modulus GQ2 multiplied by one or more other prime factors congruent to 1 (mod 4). First of all, prime factors congruent to 3 (mod 4) are produced. Then, if $e > 0$, prime factors congruent to 1 (mod 4) are produced..

For the efficacy of the construction of GQ2 moduli, it is definitely better to select each candidate before seeking to find out if it is a prime value.

Referenced by $g_1 g_2 \dots$, the base numbers are found typically among the first prime numbers: 2, 3, 5, 7, ... If there are no indications to the contrary, the m base numbers are the m first prime numbers: $g_1 = 2$, $g_2 = 3$, $g_3 = 5$, $g_4 = 7$, ... However, the following points must be noted: 2 must be avoided if a factor congruent with 5 (mod 8) is anticipated; 3 must be

avoided if the public key $\langle 3, n \rangle$ has to be used as the RSA public verification key.

Choice of $f-e$ prime factors congruent with 3 (mod 4)

On the basis of the second factor, the program requests and uses one base number per factor. For the choice of the last factor congruent with 3 (mod 4), the program finds out if there are other base numbers, namely if m is equal to or greater than $f-e$ and then, if this is the case, requests and takes account of the last base numbers, from g_{f-e} to g_m . To formalize the choice of the prime factors congruent with 3 (mod 4), we have introduced a notion of the **profile**. The profile characterizes an integer g with respect to a set of prime factors greater than g and congruent with 3 (mod 4).

- When an integer g has the same Legendre symbol with respect to two prime factors, it is said that the prime factors are equivalent with respect to g . Else, they are complementary with respect to g .
- Referenced by $\text{Profile}(g)$, the **profile** of an integer g with respect to f prime factors $p_1 p_2 \dots p_f$ is a sequence of f bits, one bit per prime factor. The first bit is equal to 1; each following bit is equal to 1 or 0 depending on whether the next factor is equivalent or complementary to p_1 with respect to g .
- When all the bits of a profile are equal to 1, it is said that the profile is flat. In such a case, all the Legendre symbols of g are equal to +1 or else to -1. When the profile of g is not flat, the equations (1) and (2) cannot be solved in x in the ring of the integers modulo n .
- By definition, the profile of g with respect to a single prime number congruent to 3 (mod 4) is always flat. This extension is used to generalize the algorithm of choice of the prime factors congruent to 3 (mod 4).

When the profiles of two base numbers g_1 and g_2 are different, which implies at least three prime factors congruent to 3 (mod 4), the knowledge

of the two private values Q_1 and Q_2 induces knowledge of two different decompositions of the modulus n . When the base numbers are small prime numbers, the program ensures that the profiles of $2^{f-e-1}-1$ multiplicative combinations of $f-e-1$ basic prime numbers are all different: they take all the possible values. The notion of profile does not extend to the prime factors congruent to 1 (mod 4).

First prime factor p_1 congruent to 3 (mod 4): each candidate must be congruent to 3 (mod 4) without any other particular constraint.

Second prime factor p_2 congruent to 3 (mod 4) with the first base number g_1 being taken into account: each candidate must be complementary to p_1 with respect to g_1 .

Third prime factor p_3 congruent to 3 (mod 4) with the second base number g_2 being taken into account: according to the profile of g_2 with respect to two first prime factors p_1 and p_2 , two cases occur. When $\text{Profile}_2(g_2)$ is flat, each candidate must be complementary to p_1 with respect to g_2 . Else, we have $\text{Profile}_2(g_1) = \text{Profile}_2(g_2)$; each candidate must then ensure that $\text{Profile}_3(g_1) \neq \text{Profile}_3(g_2)$.

Choice of i -th prime factor p_{i+1} congruent to 3 (mod 4) with the base number g_i being taken into account: according to the profile of g_i with respect to i first prime factors p_1, p_2, \dots, p_i , two cases occur. When $\text{Profile}_i(g_i)$ is flat, each candidate must be complementary to p_1 with respect to g_i . Else, among the $i-1$ base numbers g_1, g_2, \dots, g_{i-1} and all their multiplicative combinations $g_1 \cdot g_2, \dots, g_1 \cdot g_2 \cdot \dots \cdot g_{i-1}$, namely $2^{i-1}-1$ integers in all, there is one and only one integer g such that $\text{Profile}_i(g_i) = \text{Profile}_i(g)$; each candidate must then ensure that $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$.

Last prime factor p_{f-e} congruent to 3 (mod 4) with the base number g_{f-e-1} and the other base numbers from g_{f-e} to g_m being taken into account: the constraints due to the base number g_{f-e-1} are taken into account as above. Furthermore, when m is equal to or greater than $f-e$, each

candidate must provide for a non-flat profile for the last base numbers, from g_{f-e} to g_m , with respect to the $f-e$ prime factors. Each candidate must be complementary to p_1 with respect to all the values of g_i for which $\text{Profile}_{f-e-1}(g_i)$ is flat.

5 **In short, the prime factors congruent to 3 (mod 4) are chosen as a function of one another.**

For i ranging from 0 to $f-e-1$, to choose the $i+1$ -th prime factor congruent to 3 (mod 4), the candidate p_{i+1} must successfully pass the following examination:

- 10 ✓ If $i > m$ or if $i = 0$, then the candidate p_{i+1} has no other constraint; it is therefore accepted.
- ✓ If $0 < i \leq m$, then the candidate p_{i+1} must take account of the i -th base number g_i . The profile $\text{Profile}_i(g_i)$ of the base number g_i with respect to the i first prime factors from p_1 to p_i is computed. Depending on the
- 15 result, one and only one of the two following cases may occur:
- If the profile is flat, then the candidate p_{i+1} must be complementary to p_1 with respect to g_i ; else, it must be rejected.
 - Else, among the $i-1$ base numbers and all their multiplicative combinations there is one and only one number that we call g such
- 20 that $\text{Profile}_i(g) = \text{Profile}_i(g_i)$; then the candidate p_{i+1} must be such that $\text{Profile}_{i+1}(g) \neq \text{Profile}_{i+1}(g_i)$; else, it must be rejected.
- ✓ If $i+1 = f-e$ and $i < m$, namely to choose the last prime factor congruent to 3 (mod 4) when there remain base numbers, from g_{f-e} to g_m , which have not yet been taken into account, the candidate p_{f-e} must take them
- 25 into account: among these base numbers, those numbers whose profile $\text{Profile}_{f-e-1}(g_i)$ is flat are chosen; the candidate p_{f-e} must be complementary to p_1 with respect to each of the base numbers thus selected; else they must be rejected.

The candidate is accepted because it has successfully undergone the

appropriate tests.

Choice of e prime factors congruent to 1 (mod 4)

To be acceptable, each candidate p congruent to 1 (mod 4) must fulfill the following conditions with respect to each base number from g_1 to g_m .

- 5 - Let us evaluate the Legendre symbol of each base number g_i with respect to p . If the symbol is equal to -1 , let us reject the candidate p and go to another candidate. If the symbol is equal to $+1$, let us continue the evaluation of the candidate. It must be noted that if an integer 2 is used as the base number, then all the candidates congruent to 5 (mod 8) must be removed: the base number 2 is incompatible with a factor congruent to 5 (mod 8).

- 10 - Let us calculate an integer $s = (p-1+2^t)/2^{t+1}$ to establish a key $\langle s, p \rangle$. Let us apply the key $\langle s, p \rangle$ to each public value G_i to obtain a result r . Two cases occur.

- 15 - If r equals g_i or $-g_i$, then $u = 0$. In this case, and in this case alone, G_i is in a cycle. A trivial case may be noted: G_i is in a cycle provided that p is congruent to 5 (mod 8) and that the Legendre symbol of g_i with respect to p is equal to $+1$. It may be recalled that $G_i = 4$ is impossible in this case.

- 20 - If r is equal to neither g_i nor $-g_i$, then $u > 0$; it must be noted that the key $\langle (p-1)/2^t, p \rangle$ converts every non-quadratic residue y into an element b which is a primitive 2^t -th root of unity. The following algorithm computes u from r and b by using two integer variables: w initialized by r and jj taking values of 2 to 2^{t-2} .

25 For i going from 1 to $t-2$, repeat the following sequence:

- Compute $w^2/G_i \pmod{p_i}$ then raise the result to the power $2^{t-i-1} \pmod{p_i}$: we must obtain $+1$ or -1 . When -1 is obtained, compute $jj = 2^i$, then replace w by $w.b^{jj} \pmod{p_i}$. When $+1$ is obtained, do nothing.

At the end of the computation, the variable w has the value g_i or $-g_i$.

Furthermore, we know that the rank of G_i in $CG(p_j)$ is divisible by $2^u/jj$ but not by $2^{u+1}/jj$, namely that jj determines the value of u by $jj = 2^{t-u}$. When v is greater than jj , namely $k > t-u$, reject the candidate and go to another candidate. When v is smaller than or equal to jj , namely $k \leq t-u$, continue the evaluation of the candidate.

When the f prime factors have been produced, the public modulus n is the product of the f prime factors p_1, p_2, \dots, p_f . The unsigned integer n can be represented by a binary sequence; this sequence complies with the constraints imposed at the beginning of a program for the size in bits and for the number of successive most significant bits at 1. The choice of the prime factors provides for the following properties of the modulus n with respect to each of the m base numbers g_1, g_2, \dots, g_m . Furthermore, the equations (1) and (2) have no solution in x in the ring of the integers modulo n . Secondly, the equation (3) has solutions in x in the ring of the integers modulo n .

In short, the prime factors congruent to 1 (mod 4) are chosen independently of one another. While the factors congruent to 3 (mod 4) gradually take account of the base numbers, each prime factor congruent to 1 (mod 4) must take account of all the constraints dictated by each of the base numbers. Each prime factor congruent with 1 (mod 4), namely p , from p_{f-e} to p_f should have successfully undergone the following examination in two steps.

1) The step (1) is executed successively for each of the m base numbers from g_1 to g_m .

The Legendre symbol of the current base number g with respect to the candidate p is computed. One and only of the following two cases arises: if the symbol is equal to -1 , the candidate is rejected. Else (the symbol is equal to $+1$), the examination is continued in passing to the base number g following the step (1).

When the candidate is acceptable for all the m base numbers, the operation passes to the step (2).

2) The step (2) is executed successively for each of the m public values of G_1 to G_m .

5 An integer t is computed such that $p-1$ is divisible by 2^t but not by 2^{t+1} , then an integer $s = (p-1+2^t)/2^{t+1}$, so as to set up a key $\langle s, p \rangle$. The key $\langle s, p \rangle$ is applied to the current public value $G = g^2$ to obtain a result r , namely: $r \equiv G^s \pmod{p}$. Depending on the result, one and only one of the following states arises:

- 10 a) If r is equal to g or to $-g$, then $u = 0$; the examination of the candidate is continued in passing to the following public value G at the step (2).
 b) Else, a positive number u is computed taking one of the values from 1 to $t-2$, in applying the following algorithm which implements two variables: jj taking values ranging from 2 to 2^{t-2} and w initialized by r , as well as an integer b obtained by applying a key $\langle (p-1)/2^t, p \rangle$ to a non-quadratic residue of $\text{CG}(p)$.

15 For an index ii ranging from 1 to $t-2$, the following operation is repeated:

20 $w^2/G \pmod{p}$ is computed and then a key $\langle 2^{t-ii-1}, p \rangle$ is applied to the result to obtain $+1$ or -1 (else, there is proof that the candidate is not a prime factor). If -1 is obtained, then $jj = 2^{ii}$ is computed and then $c \equiv b^{jj} \pmod{p}$, and then w is replaced by $w \cdot c \pmod{p}$, then there is a passage to the next index ii . If $+1$ is obtained, there is a passage to the next index ii .

25 At the end of the algorithm, the value in the variable jj defines u by the relationship $jj = 2^{t-u}$; the value in the variable w is a square root of G , namely g or $-g$ (else, there is proof that the candidate is not a prime factor). Two cases occur:

- If $t-u < k$, then the candidate p is rejected because the branch

where G occurs is not long enough.

- If $(t-u \geq k)$, the evaluation of the candidate is continued in going to the next public value G following the step (2).

When the candidate is acceptable for all the m public values, it is accepted as a prime factor congruent with 1 (mod 4).

Computation of the associated values

To obtain the private components, let us first calculate all the solutions to the equation (3.a) in the two simplest and most current cases before taking up the general case.

For each prime factor p_j congruent to 3 (mod 4), the key $\langle (p_j+1)/4, p_j \rangle$ gives the quadratic square root of any quadratic residue. From this, a method is deduced for computing a solution to the equation (3.a):

$$s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2}; \text{ then, } Q_{ij} \equiv G_i^{s_j} \pmod{p_j}$$

or else rather the inverse (mod p_j) of such a solution.

$$s_j \equiv (p_j-1)/2 - ((p_j+1)/4)^k \pmod{(p_j-1)/2}; \text{ then, } Q_{ij} \equiv G_i^{s_j} \pmod{p_j}$$

In $\text{CG}(p_j)$, there are then two and only two square roots of unity: +1 and -1; there are therefore two solutions in x to the equation (3.a): the two numbers Q_{ij} and $p_j - Q_{ij}$ are the same square $G_i \pmod{p_j}$.

For each prime factor p_j congruent to 5 (mod 8), the key $\langle (p_j+1)/4, p_j \rangle$ gives the odd-parity ranking square root of any odd-parity ranking element. From this, a solution to the equation (3.a) is deduced:

$$s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}; \text{ then, } Q_{ij} \equiv G_i^{s_j} \pmod{p_j}$$

or else rather the inverse (mod p_j) of such a solution.

$$s_j \equiv (p_j-1)/4 - ((p_j+3)/8)^k \pmod{(p_j-1)/4}; \text{ then } Q_{ij} \equiv G_i^{s_j} \pmod{p_j}$$

In $\text{CG}(p_j)$, there are then four and only four fourth roots of unity; there are therefore four solutions in x to the equation (3.a). Let us note that $2^{(p_j-1)/4} \pmod{p_j}$ is a square root of -1 because the Legendre symbol of 2 with respect to p congruent to 5 (mod 8) is equal to -1. If Q_{ij} is a solution, then $p_j - Q_{ij}$ is another solution, as well as the product (mod p_j) of Q_{ij} by a square

root of -1 .

For a prime factor p_j congruent to $2^{t+1} \pmod{2^{t+1}}$, the key $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ gives the odd parity square root of any odd-parity ranking element. It is therefore possible to compute a solution to the equation (3.a).

- Let us first of all compute an integer $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$ to set up a key $\langle s_j, p_j \rangle$.
- When the key $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ converts G_i into g_i or into $-g_i$, the rank of G_i is an odd-parity value in $\text{CG}(p_j)$ ($u = 0$). Then, the key $\langle s_j, p_j \rangle$ converts G_i into a number z : this is the odd-parity ranking solution to the equation (3.a). According to the values of t and k , there is still $\min(2^k-1, 2^t-1)$ other solutions on one or more branches. The branch of z^2 carries another solution: this is p_j-z . When $t \geq 2$, the branch of z^4 has two other solutions: it is the product of z by each of the two square roots of -1 , namely each of the two primitive fourth roots of unity. Now, if y is a non-quadratic residue of $\text{CG}(p_j)$, then $y^{(p_j-1)/4} \pmod{p_j}$ is a square root of -1 . In general, for i taking each value of 1 to $\min(k, t)$, the branch of the 2^i -th power of z bears 2^{i-1} solutions: these are the products $\pmod{p_j}$ of z by each of the 2^{i-1} primitive 2^i -th roots of unity. Now if y is a non-quadratic residue of $\text{CG}(p_j)$, then y to the power $(p_j-1)/2^i$ is a 2^i -th primitive root of unity that we call c . The 2^{i-1} to 2^i -th primitive roots of unity are the odd parity powers of c : $c, c^3 \pmod{p_j}, c^5 \pmod{p_j}, \dots c$ to the power $2^i-1 \pmod{p_j}$.
- When the key $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ converts G_i into an integer r that is neither g_i nor $-g_i$, the rank of G_i is an even-parity value in $\text{CG}(p_j)$ ($u > 0$). Then, provided that G_i is appropriately placed in a fairly lengthy branch, namely $t \geq k + u$, there are 2^k solutions on the branch where G_i is located. To compute a 2^k -th root, it is enough to reiterate the above-stated square root computation algorithm k rank times, so as to compute

the square root of the successive results up to a solution z . This computation may of course be optimized to directly approach a 2^k th root and then adjust the approximation of a 2^k -th root in a single operation to achieve a solution z . To obtain all the other solutions, it may be noted first of all that if y is a non-quadratic residue of $CG(p_i)$, then y to the power $(p_i-1)/2^k$ is a primitive 2^k -th root of unity which we shall call d . The 2^k 2^k -th roots of unity are successive powers of d : $d, d^2 \pmod{p_i}, d^3 \pmod{p_i}, \dots d$ to the power of $2^k-1 \pmod{p_i}$, d to the power $2^k \pmod{p_i}$ equal to 1. The 2^k solutions on the branch where G_i is located are the products $\pmod{p_i}$ of z for each of these roots.

In short, to compute a component for the prime factor p and the base number g , with k, t and u being known, the following procedure is used:

- 1) An integer is computed: $s \equiv ((p-1+2^t)/2^{t+1})^k \pmod{(p-1)/2^t}$ to set up a key $\langle s, p \rangle$. Then, the key $\langle s, p \rangle$ is applied to G to obtain $z \equiv G^s \pmod{p}$. According to the value of u , there is a passage to the step (2) or (3).
- 2) If $u = 0$, z is the odd-parity solution to the equation (3.a). There are still $\min(2^k-1, 2^t-1)$ other even-parity ranking solutions on one or more branches, very precisely on $\min(k, t)$ other branches. For i ranging from 1 to $\min(k, t)$, the branch of the 2^i -th power of z has 2^{t-1} solutions: these are the products \pmod{p} of z by each of 2^{t-1} 2^i -th primitive roots of unity. The generic solution to the equation (3.a) is shown by zz . The operation goes to the step (4).
- 3) If $u > 0$, all the solutions to the equation (3.a) are even-parity solutions. There are 2^k of them and they are all in the branch on which G is located; indeed: $t-u \geq k$. To compute a solution, the following algorithm implements two variables: jj assuming values ranging from 2 to 2^{t-2} and w initialized by z , as well as an integer b obtained by applying a key $\langle (p-1)/2^t, p \rangle$ to a non-quadratic residue of $CG(p)$.

The following sequence is repeated k ranking times.

For an index ii ranging from 1 to $t-2$, the following operation is repeated: $w^2/G \pmod{p}$ is computed and then a key $\langle 2^{t-ii-1}, p \rangle$ is applied to the result to obtain +1 or -1 (else there is proof that p is not a prime number). If -1 is obtained, then $jj = 2^{ii}$ is computed, then $c \equiv b^{jj} \pmod{p}$, then w is replaced by $w.c \pmod{p}$, then there is a passage to the next index ii . If +1 is obtained, there is a passage to the next index ii .

At the end of the algorithm, the variable w has the value za . The 2^k solutions on the branch where G is located are the products \pmod{p} of za by each of the 2^k -th roots of unity. The generic solution to the equation (3.a) is represented by zz . The operation passes to the step (4).

- 4) With zz being known, a component value is deduced therefrom: it is the inverse of zz modulo p when the equation $G.Q^v \equiv 1 \pmod{n}$ is used and zz when the equation $G \equiv Q^v \pmod{n}$ is used.

Note. There are various methods to obtain the private components and the private values. If a collection of f components is known, namely the f components for a given base number, the Chinese remainder technique is used to compute the corresponding private value. It can be seen that for a given public value G and a modulus n , it is possible to have several possible private values Q . There are four of them when n is the product of two prime factors congruent to 3 $\pmod{4}$; there are eight of them with three prime factors congruent to 3 $\pmod{4}$; there are sixteen of them with two prime factors congruent to 3 $\pmod{4}$ and one congruent to 5 $\pmod{8}$. A judicious use of these multiple values may complicate the attacks by analysis of the electrical consumption of a chip card using GQ2.

Thus, as and when t increases, the program gets complicated for increasingly rare cases. Indeed, the prime numbers are distributed on an

average as follows: $t = 1$ for one in two, $t = 2$ for one in four, $t = 3$ for one in eight and so on and so forth. Furthermore, the constraints due to m base numbers make the candidacies increasingly unacceptable. Whatever the case may be, the combined moduli definitively form part of GQ2 technology; the type of GQ2 modulus in no way affects the dynamic authentication and digital signature protocols.

Figure 3 illustrates $G_i = g_i^2$ in a cycle with a prime factor p congruent to 9 (mod 16), namely $t = 3$, $u = 0$, as well as $k \geq 3$. It may be noted that:

$$b \equiv y^{\frac{p-1}{8}} \pmod{p}$$

$$b^8 \equiv 1 \pmod{p}$$

$$b^4 \equiv -1 \pmod{p}$$

Figure 4 illustrates $G_i = g_i^2$ on a branch with a prime factor p congruent to 65 (mod 128), namely $t = 6$ as well as $k = 4$ and $u = 2$.

Here is a first set of keys GQ2 with $k = 6$, giving $v = 64$, $m = 3$, giving three base: $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, and $f = 3$, namely a modulus with three prime factors: two congruent to 3 (mod 4) and one to 5 (mod 8). It must be noted that $g = 2$ is incompatible with a prime factor congruent to 5 (mod 8).

$p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833$

$(2 | p_1) = -1 ; (3 | p_1) = +1 ; (5 | p_1) = -1 ; (7 | p_1) = +1$

$p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B$

$(2 | p_1) = -1 ; (3 | p_1) = -1 ; (5 | p_1) = +1 ; (7 | p_1) = -1$

$p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD$

$(2 | p_1) = -1 ; (3 | p_1) = +1 ; (5 | p_1) = +1 ; (7 | p_1) = +1$

$n = p_1 \cdot p_2 \cdot p_3 = \text{FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9}$
 $02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144$
 $CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD$

$Q_{1,1} = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE$

$Q_{2,1} = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89$

$$Q_{3,1} = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F$$

$$Q_{1,2} = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502$$

$$Q_{2,2} = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E$$

$$Q_{3,2} = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E$$

$$5 \quad Q_{1,3} = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE$$

$$Q_{2,3} = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877$$

$$Q_{3,3} = 01682D490041913A4EA5B80D16B685E4A6DD88070501$$

$$Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8$$

$$C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A$$

$$10 \quad C74D9743435AB4D7CF0FF6557$$

$$Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4$$

$$DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8$$

$$82288273ADE67353A5BC316C093$$

$$Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A$$

$$15 \quad AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197$$

$$697238537FE7A0195C5E8373EB74D$$

The following are other possible values for the components related to the p_3 which is congruent to 5 (mod 8).

$$20 \quad \text{The following is a square root of } -1 \text{ in } \text{CG}(p_3) : c = 2^{(p_3-1)/4} \pmod{p_3} =$$

$$0C3000933A854E4CB309213F12CAD59FA7AD775AAC37$$

$$Q'_{1,3} = c \cdot Q_{1,3} \pmod{p_3} =$$

$$050616671372B87DEC9AEEAC68A3948E9562F714D76C$$

$$Q'_{2,3} = c \cdot Q_{2,3} \pmod{p_3} =$$

$$25 \quad 06F308B529C9CE88D037D01002E7C838439DACC9F8AA$$

$$Q'_{3,3} = c \cdot Q_{3,3} \pmod{p_3} =$$

$$015BE9F4B92F1950A69766069F788E45439497463D58$$

Giving:

$$Q'_1 = 676DF1BA369FF306F4A1001602BCE5A008DB82882E87C148D0$$

$$30 \quad D820A711121961C9376CB45C355945C5F2A9E5AFAAD7861886284A$$

9B319F9E4665211252D74580

$Q'_2 = \text{CAEC4F41752A228CF9B23B16B3921E47C059B9E0C68634C2C}$
 $64\text{D6003156F30EF1BC02ADA25581C8FDE76AA14AB5CC60A2DE1C}$
 $565560B27E8AA0E6F4BCA7FE966$

5 $Q'_3 = 2\text{ACDF5161FE53B68CC7C18B6AFE495815B46599F44C51A6A1}$
 $\text{A4E858B470E8E5C7D2200EF135239AF0B7230388A6A5BDD8EE15B}$
 $0\text{D094FC2BFA890BFDA669D9735}$

The following is a second set of keys GQ2, with $k = 9$, that is $v = 512$, $m = 2$, that is
 two base numbers: $g_1 = 2$ and $g_2 = 3$, and $f = 3$, giving a modulus with three prime
 10 factors congruent to 3 (mod 4).

$p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB$

$(2 | p_1) = -1$; $(3 | p_1) = -1$; and we get: $(6 | p_1) = +1$.

$p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7$

$(2 | p_2) = +1$; $(3 | p_2) = -1$; and we get: $(6 | p_2) = -1$.

15 $p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3$

$(2 | p_3) = -1$; $(3 | p_3) = +1$; and we get : $(6 | p_3) = -1$.

$n = p_1 \cdot p_2 \cdot p_3 = \text{FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D}$
 $6698\text{AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49}$
 $761\text{B276A8E6B6977A21D51669D039F1D7}$

20 $Q_{1,1} = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1$

$Q_{2,1} = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E$

$Q_{1,2} = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A$

$Q_{2,2} = 045ECB881387582E7C556887784D2671CA118E22FCF2$

$Q_{1,3} = \text{B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982}$

25 $Q_{2,3} = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB$

$Q_1 = 27\text{F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C}$
 $35\text{F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6}$
 $\text{EDDA092D0CF108D0AB708405DA46}$

$Q_2 = 230\text{D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64}$
 30 $9\text{C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6}$

F11F19874DE7DC5D1DF2A9252D

The present application has described a method for the production of sets of GQ2 keys, namely moduli n and pairs of public and private values G and Q respectively, in which the exponent v is equal to 2^k . These sets of keys are used to implement a method designed to prove the authenticity of an entity and/or the integrity and/or the authenticity of a message as has been described.

In the pending applications filed on the same day by France Télécom, TDF and the firm Math RiZK, and whose inventors are Louis Guillou and Jean-Jacques Quisquater, the characteristic features of the methods, systems and devices designed to prove the authenticity of an entity and/or the integrity and/or the authenticity of a message have been claimed. These two applications are incorporated herein by reference.

CLAIMS

1. In a method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity.

by means of all or part of the following parameters or derivatives of these parameters:

- a public modulus n constituted by the product of f prime factors p_1, p_2, \dots, p_f (f being equal to or greater than 2),

- a public exponent v ;

- m distinct integer base numbers g_1, g_2, \dots, g_m (m being greater than or equal to 1), the base numbers g_i being such that:

the two equations (1) and (2):

$$x^2 \equiv g_i \pmod{n} \quad \text{and} \quad x^2 \equiv -g_i \pmod{n}$$

cannot be resolved in x in a ring of integers modulo n ,

and such that:

the equation (3):

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of integers modulo n .

the method according to the invention making it possible to produce the f prime factors p_1, p_2, \dots, p_f in such a way that the equations (1), (2) and (3) are satisfied, said method comprising the step of choosing firstly:

- the m base numbers g_1, g_2, \dots, g_m ,

- the size of the modulus n ,

- the size of the f prime factors p_1, p_2, \dots, p_f .

2. Method according to claim 1 such that, when the public exponent v has the form:

$$v = 2^k$$

where k is a security parameter greater than 1, the security parameter k is

also chosen as a prime number.

3. Method according to one of the claims 1 or 2, such that the m base numbers $g_1, g_2, \dots g_m$, are chosen at least partly among the first integers.

4. Method according to one of the claims 2 or 3, such that the security parameter k is a small integer, especially smaller than 100.

5. Method according to one of the claims 1 to 4, such that the size of the modulus n is greater than several hundreds of bits.

6. Method according to one of the claims 1 to 5, such that the f prime factors $p_1, p_2, \dots p_f$ have a size close to the size of the modulus n divided by the number f of factors..

7. Method according to one of the claims 1 to 6 such that, among the f prime factors $p_1, p_2, \dots p_f$,

- a number e of prime factors congruent to 1 modulo 4 is chosen, e possibly being zero (should e be zero, the modulus n will hereinafter be called a basic modulus, should $e > 0$, the modulus n will hereinafter be called a combined modulus),

- the $f-e$ other prime factors are chosen to be congruent to 3 modulo 4, $f-e$ being at least equal to 2.

8. A method according to claim 7 such that, to produce the $f-e$ prime factors $p_1, p_2, \dots p_{f-e}$ congruent to 3 modulo 4, the following steps are implemented:

- the first prime factor p_1 congruent to 3 modulo 4 is chosen and then,
- the second prime factor p_2 is chosen such that p_2 is complementary to p_1 with respect to the base number g_1 .

- the factor p_{i+1} is chosen in carrying out the following procedure in, distinguishing two cases:

(1) the case where $i > m$

- the factor p_{i+1} congruent to 3 modulo 4 is chosen.

(2) Case where $i \leq m$

- the Profile ($\text{Profile}_i(g_i)$) of g_i with respect to the i first prime factors p_i is computed:

- if the $\text{Profile}_i(g_i)$ is flat, the factor p_{i+1} is chosen such that p_{i+1} is complementary to p_i with respect to g_i ,

5 - else, among the $i-1$ base numbers g_1, g_2, \dots, g_{i-1} and all their multiplicative combinations, the number, hereinafter called g , is chosen such that $\text{Profile}_i(g) = \text{Profile}_i(g_i)$, and then p_{i+1} is chosen such that $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$.

10 (the terms "complementary", "profile", "flat profile" having the meanings defined in the description).

9. A method according to claim 8 such that, to choose the last prime factor p_{f-e} , the following procedure is used in distinguishing three cases:

(1) Case where $f-e-1 > m$

15 • p_{f-e} is chosen congruent to 3 modulo 4.

(2) Case where $f-e-1 = m$

• $\text{Profile}_{f-e-1}(g_m)$ is computed with respect to the $f-e-1$ first prime factors from, p_1 to p_{f-e-1} ,

20 • • if $\text{Profile}_{f-e-1}(g_m)$ is flat, p_{f-e-1} is chosen such that it is complementary to p_1 with respect to g_m ,

• • else:

• • • among the $m-1$ base numbers from g_1 to g_{m-1} and all their multiplicative combinations, the number hereinafter called g is chosen such that $\text{Profile}_i(g) = \text{Profile}_i(g_i)$,

25 • • • then p_{f-e} is chosen such that $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$.

(3) Case where $f-e-1 < m$

• p_{f-e} is chosen such that the following two conditions are met:

(3.1) First condition

• **Profile_{f-e-1}(g_{f-e-1})** is computed with respect to the f-e-1 first prime factors from **p₁** to **p_{f-e-1}**,

• • If **Profile_{f-e-1}(g_{f-e-1})** is flat, **p_{f-e}** is chosen so that it meets the first condition of being complementary to **p₁** with respect to

g_{f-e-1}.

• • Else,

• • • among the f-e-1 base numbers from **g₁** to **g_{m-1}** and all their multiplicative combinations, the number, hereinafter called **g** is chosen such that **Profile₁(g) =**

Profile_{f-e-1}(g_{f-e-1}),

• • • then **p_{f-e}** is chosen so that it meets the first condition of being such that **Profile_{f-e}(g) ≠ Profile_{f-e}(g_m)**,

(3.2) Second condition

• among all the last base numbers from **g_{f-e}** to **g_m**, those numbers whose Profile **Profile_{f-e-1}(g_i)** is flat are chosen and then

• **p_{f-e}** is chosen so that it meets the second condition of being complementary to **p₁** with respect to each of the base numbers thus selected.

10. Method according to the claims 8 or 9 such that, to produce the e prime factors congruent to 1 modulo 4, each prime factor candidate **p** is evaluated, from **p_{f-e}** to **p_f**, in being subjected to the following two successive tests:

(1) First test

- the Legendre symbol is computed for each base number **g_i**, from **g₁** to **g_m**, with respect to the candidate prime factor **p**,

• if the Legendre symbol is equal to -1, the candidate **p** is rejected,

• if the Legendre symbol is equal to +1, the evaluation of the candidate **p** is continued in passing to the following base

number and then, when the last base number has been taken into account, there is a passage to the second test.

(2) Second test

- an integer number t is computed such that $p-1$ is divisible by 2^t , but not by 2^{t+1} , then

- an integer s is computed such that $s = (p-1+2^t)/2^{t+1}$.

- the key $\langle s, p \rangle$ is applied to each public value G_i to obtain a result r

$$r \equiv G_i^s \pmod{p}$$

• if r is equal to g_i or $-g_i$, the second test is continued in passing to the following public value G_{i+1} .

• if r is different from g_i or $-g_i$, a factor u is computed in applying the following algorithm:

• • the algorithm consists of the repetition of the following sequence specified for an index ii ranging from 1 to $t-2$:

• • the algorithm implements two variables: w initialized by r and $jj = 2^{ii}$ assuming values ranging from 2 to 2^{t-2} , as well a number b obtained by application of the key $\langle (p-1)/2^t, p \rangle$ to a non-quadratic residue of $CG(p)$, then the following steps 1 and 2 are iterated:

• • • Step 1: $w^2/G_i \pmod{p}$ is computed,

• • • Step 2: the result is raised to the power of 2^{t-ii-1} .

• • • • If $+1$ is obtained, the second test is continued in passing to the following public value G_{i+1} ,

• • • • If -1 is obtained, $jj = 2^{ii}$ is computed and then w is replaced by $w.b^{jj} \pmod{p}$, then the algorithm is continued for the following value having an index ii .

•• at the end of the algorithm, the value in the variable jj is used to compute an integer u by the relation $jj = 2^{t-u}$ and then the expression $t-u$ is computed. Two cases arise:

••• if $t-u < k$, the candidate p is rejected

••• if $t-u > k$, the evaluation of the candidate p is continued in continuing the second test and in passing to the following public value G_{i+1} , the candidate p is accepted as a prime factor congruent to 1 modulo 4 if, at the end of the second test, for all the m public values G_i , it has not been rejected.

11. Method applying the method according to any of the claims 1 to 10, making it possible to produce f prime factors p_1, p_2, \dots, p_f , this method being designed to prove the following to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),

- the public modulus n constituted by the product of said prime factors $f p_1, p_2, \dots, p_f$ (f being greater than or equal to 2),

- the public exponent v ;

said modulus, said exponent and said values being linked by relations of the following type:

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

said exponent v being such that

$$v = 2^k$$

where k is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than

the f prime factors p_1, p_2, \dots, p_f , the base number g_i being such that:
the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo n
and such that:

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n .

said method implements, in the following steps, an entity called a witness
having f prime factors p_i and/or parameters of the Chinese remainders of the
prime factors and/or of the public modulus n and/or the m private values Q_i
and/or $f \cdot m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and
of the public exponent v ;

- the witness computes commitments R in the ring of integers modulo
 n ; each commitment being computed:

- either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random factor such that $0 < r < n$,

- or

- • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random factors $\{r_1, r_2, \dots, r_f\}$,

- • then by applying the Chinese remainder method;

- the witness receives one or more challenges d , each challenge d
comprising m integers d_i hereinafter called elementary challenges; the
witness, on the basis of each challenge d , computing a response D ,

- either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

• • and then by applying the Chinese remainder method.

5 said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R**, **d**, **D** forming a triplet referenced **{R, d, D}**.

10 **12.** A method according to claim 11 such that to implement the pairs of private values **Q₁, Q₂, ... Q_m** and public values **G₁, G₂, ... G_m** as just described, the method uses the prime factors **p₁, p₂, ... p_r** and/or the parameters of the Chinese remainders, the base numbers **g₁, g₂, ... g_m** and/or the public values **G₁, G₂, ... G_m** to compute:

15 - either the private values **Q₁, Q₂, ... Q_m** by extracting a **k**-th square root modulo **n** of **G_i**, or by taking the inverse of a **k**-th square root modulo **n** of **G_i**,

- or the **f.m** private components **Q_{i,j}** of the private values **Q₁, Q₂, ... Q_m** such that **Q_{i,j} ≡ Q_i (mod p_j)**.

13. A method according to claim 12 such that, to compute the **f.m** private components **Q_{i,j}** of the private values **Q₁, Q₂, ... Q_m**:

20 - the key **<s, p_j>** is applied to compute **z** such that:

$$z \equiv G_i^s \bmod p_j$$

- and the values **t** and **u** are used.

- computed as indicated here above when **p_j** is congruent to 1 modulo 4 and

25 • taken to be respectively equal to 1 (**t=1**) and 0 (**u=0**) where **p_j** is congruent to 3 modulo 4.

• • if **u** is zero, we consider all the numbers **zz** such that:

• • • **zz** is equal to **z** or such that

• • • **zz** is equal to a product (mod **p_j**) of **z** by each of

the 2^{ii-t} 2^{ii} -th primitive roots of unity, ii ranging from 1 to $\min(k,t)$.

• • If u is positive, we consider all the numbers zz such that zz is equal to the product (mod p_j) of za by each of the 2^k 2^k -th roots of unity, za designating the value of the variable w at the end of the algorithm implemented in claim 10,

- at least one value of the component $Q_{i,j}$ is deduced therefrom, it is equal to zz when the equation $G_i \equiv Q_i^v \bmod n$ is used or else it is equal to the inverse of zz modulo p_j of zz when the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ is used.

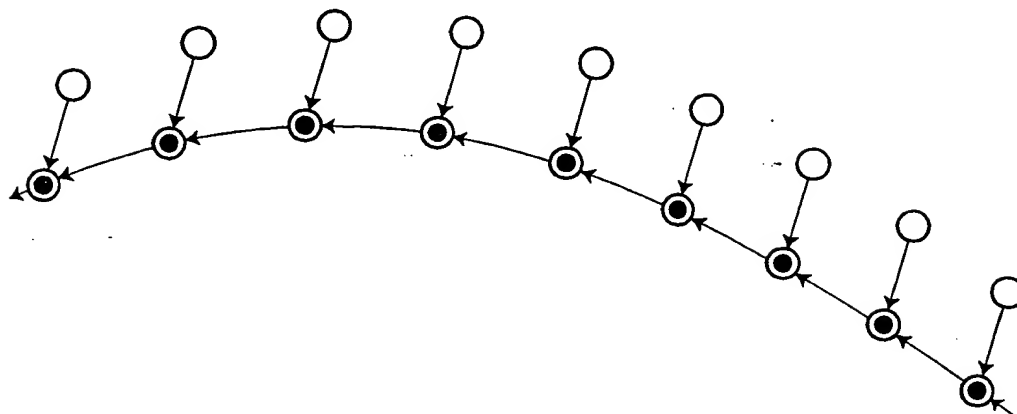


Fig.1A

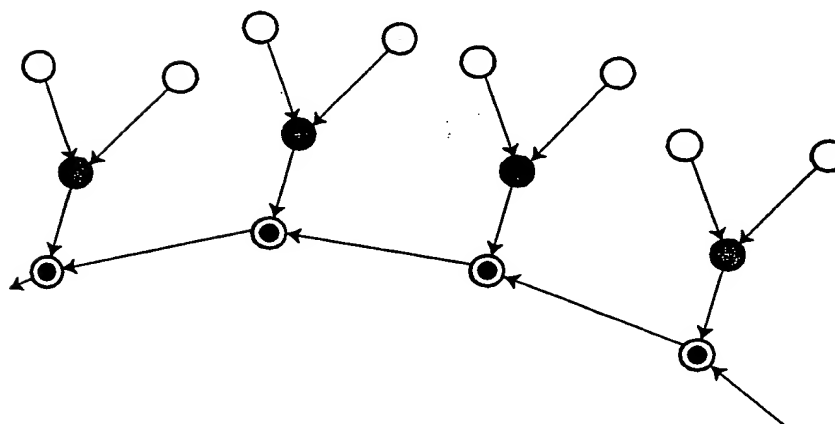


Fig.1B

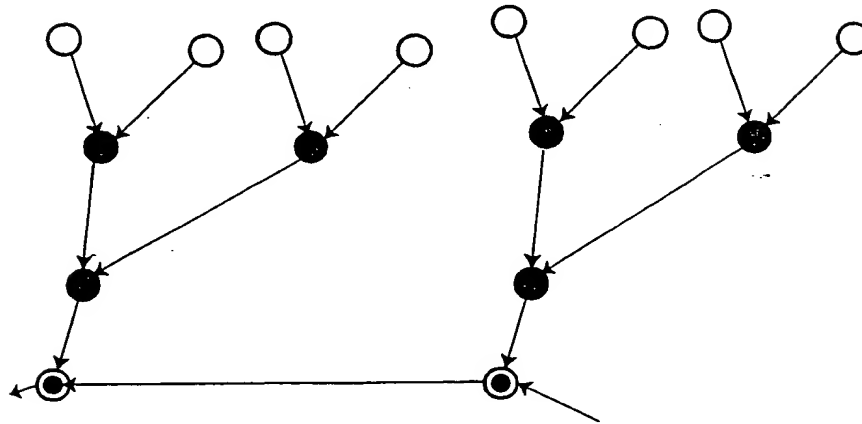


Fig.1C

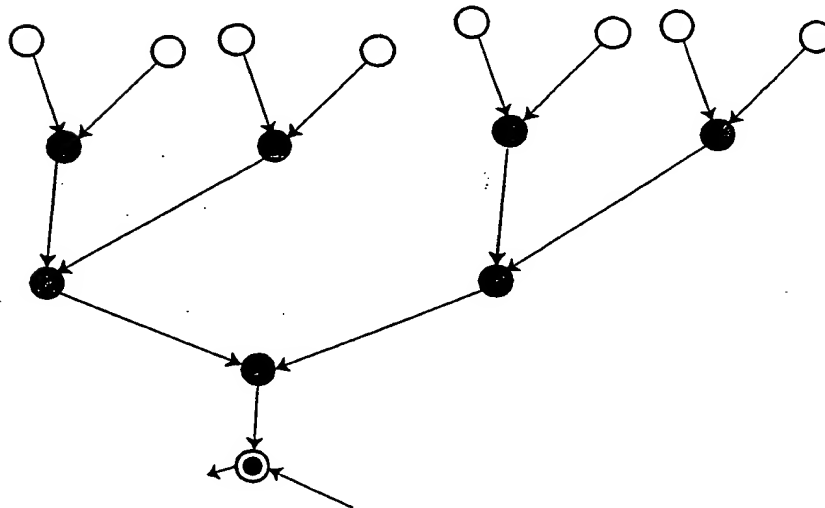


Fig.1D

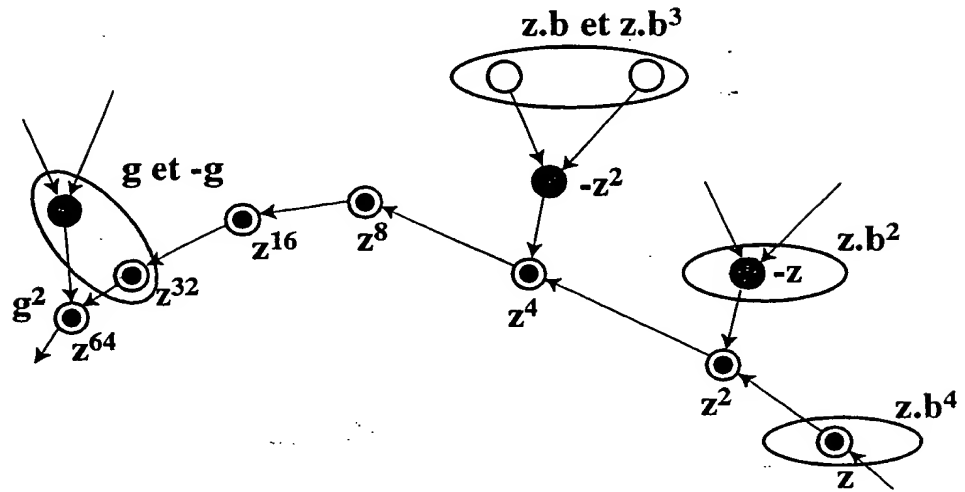


Fig.2

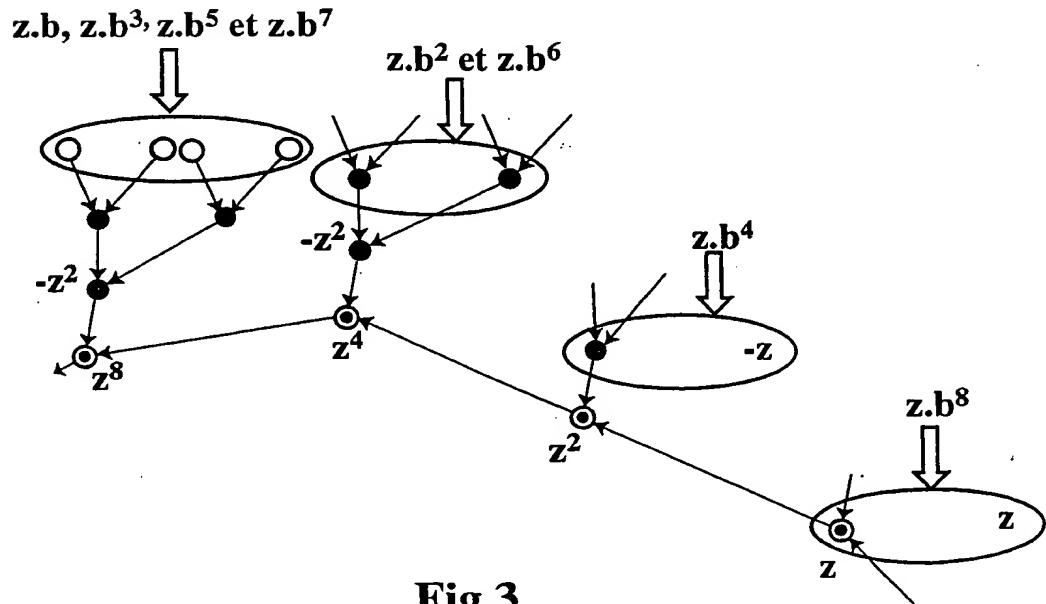


Fig.3

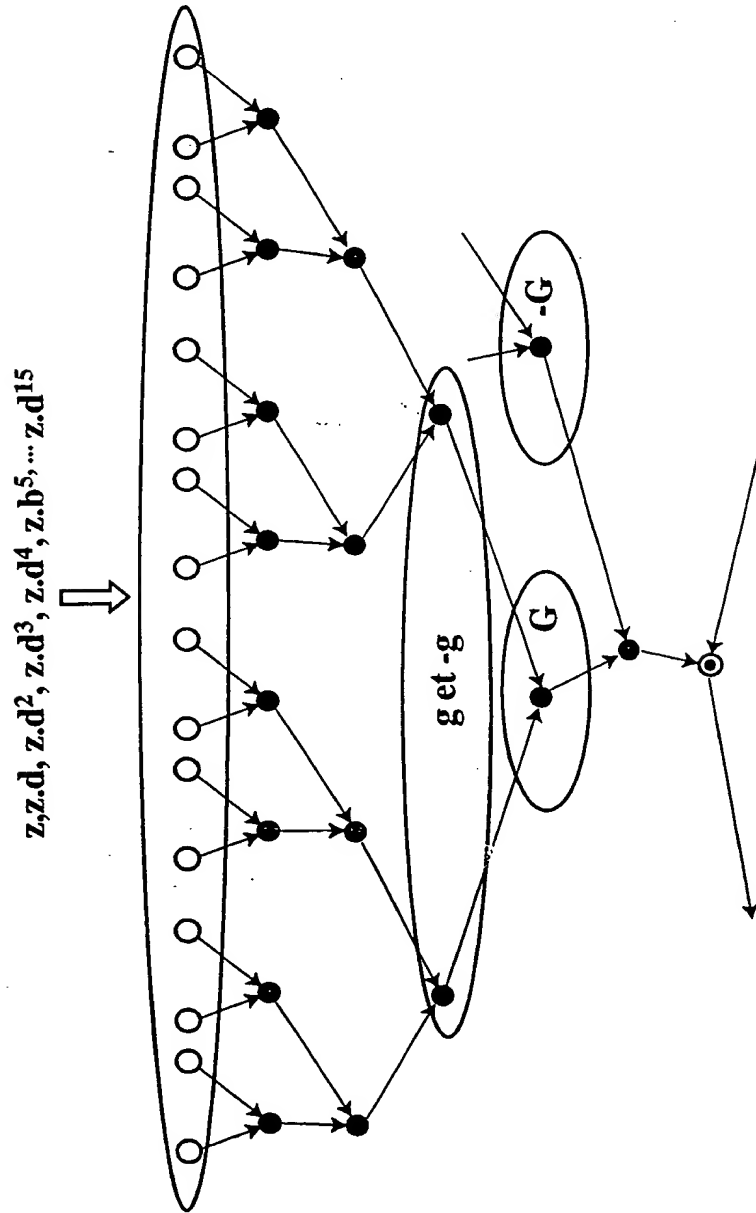


Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT /FR00/00190

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/32

International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 August 1997 (1997-08-27) column 9, line 39- column 12, line 38 figure 3 ---	1,6,11, 12,15 2,7,16.
A	WO 96 33567 A (GEMPLUS CARD INT; NACCACHE DAVID (FR)) 24 October 1996 (1996-10-24) Page 2, line 27 -page 4, line 12 Page 15, line 31 -page 18, line 17 ---	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 November 1989 (1989-11-30) page 10, line 2-page 11, line 6 page 12, line 21-page 14, line 6 ---	3,4,8,9, 13,14, 17,18

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
28 March 2000 (28.03.00)

Date of mailing of the international search report
19 April 2000 (19.04.00)

Name and mailing address of the
EUROPEAN PATENT OFFICE

Authorized officer

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No

PCT/FR 00/00190

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0792044	A	27-08-1997	JP	10247905 A	14-09-1998
			US	5987134 A	16-11-1999
WO 9633567	A	24-10-1996	FR	2733378 A	25-10-1996
			FR	2733379 A	25-10-1996
			EP	0766894 A	09-04-1996
			JP	10506727 T	30-06-1998
			US	5910989 A	08-06-1999
WO 8911706	A	30-11-1989	AU	622915 B	30-04-1992
			AU	3733589 A	12-12-1989
			CA	1321649 A	24-08-1993
			EP	0374225 A	27-06-1990
			JP	2504435 T	13-12-1990
			US	4935962 A	19-06-1990
EP 0311470	A	12-04-1989	FR	2620248 A	10-03-1989
			AT	83573 T	15-01-1993
			AU	2197188 A	23-03-1989
			CA	1295706 A	11-02-1992
			DE	3876741 A	28-01-1993
			FI	884082 A, B,	08-03-1989
			JP	1133092 A	25-05-1989
			KR	9608209 B	20-06-1996
			US	5218637 A	08-06-1993
			US	5140634 A	18-08-1992

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 00/00190

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27) colonne 9, ligne 39 -colonne 12, ligne 38 figure 3	1,6,11, 12,15 2,7,16
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24) page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30) page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6	3,4,8,9, 13,14, 17,18
	-/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

28 mars 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 851 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Masche, C

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR 00/00190

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0792044	A	27-08-1997	JP 10247905 A	14-09-1998
			US 5987134 A	16-11-1999
WO 9633567	A	24-10-1996	FR 2733378 A	25-10-1996
			FR 2733379 A	25-10-1996
			EP 0766894 A	09-04-1996
			JP 10506727 T	30-06-1998
			US 5910989 A	08-06-1999
WO 8911706	A	30-11-1989	AU 622915 B	30-04-1992
			AU 3733589 A	12-12-1989
			CA 1321649 A	24-08-1993
			EP 0374225 A	27-06-1990
			JP 2504435 T	13-12-1990
			US 4935962 A	19-06-1990
EP 0311470	A	12-04-1989	FR 2620248 A	10-03-1989
			AT 83573 T	15-01-1993
			AU 2197188 A	23-03-1989
			CA 1295706 A	11-02-1992
			DE 3876741 A	28-01-1993
			FI 884082 A, B,	08-03-1989
			JP 1133092 A	25-05-1989
			KR 9608209 B	20-06-1996
			US 5218637 A	08-06-1993
			US 5140634 A	18-08-1992